
ORADOR DESCONOCIDO: Buenos días, buenas tardes y buenas noches a todos. bienvenidos a este webinar de At-Large sobre el tema del equipo del PDP expeditivo, sobre el desarrollo de políticas sobre la especificación temporaria para los datos de registración sobre gTLD fase dos, que ocurre este lunes 6 de abril de 2020 a las 20:00 UTC.

No vamos a pasar la lista porque se trata de un seminario web. Quisiera recordarles a todos que digan su nombre antes de tomar la palabra. Quiero recordarles a todos los participantes en el teléfono y en la computadora que pongan en silencio sus micrófonos cuando no estén hablando y que digan su nombre cuando toman la palabra, no solo para la transcripción sino también para que los intérpretes los identifiquen adecuadamente. En esta llamada tenemos interpretación al inglés, al español y al francés. También transcripción en tiempo real en inglés. Les voy a dar el link en el chat. Les agradezco por participar y le doy la palabra a Joanna Kulesza, la presidenta de este grupo de trabajo.

JOANNA KULESZA: Muchas gracias. En nombre de Alfredo y de mí misma quiero agradecerles por participar de este webinar que ha sido coordinado y organizado por Hadia Elminiawi, quien está en realidad liderando un pequeño subgrupo sobre generación de capacidad y seminarios web. Muchas gracias, Hadia, por establecer esta llamada. Sé que tenemos un plan de una serie de seminarios web y también me gustaría darles la bienvenida a todos y agradecerles por tomarse el tiempo de participar.

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.

En los próximos 90 minutos, Hadia y Alan nos van a dar una actualización sobre el proceso del EPDP. En la lista de participantes veo que tenemos muchos embajadores de ATLAS III. El ejercicio del ATLAS III en buena medida se focalizaba en el EPDP como ejemplo de cómo se está desarrollando el proceso de políticas dentro de la comunidad de la ICANN. Para aquellos que han participado y han seguido nuestro seminario web, que hemos ido organizando y que llevaron hasta esta reunión, esta va a ser una actualización. Para aquellos que son muy nuevos en el desarrollo de políticas de la ICANN, el EPDP es un proceso desafiante pero al mismo tiempo muy interesante, muy innovador, que resulta un intento para ese marco global de los registradores y registratarios de nombres de dominio en la política local.

Se trata de un tema muy interesante, desafiante también, como decía. Al mismo tiempo, At-Large está siendo representada por Hadia y Alan, que le han dedicado mucho tiempo, mucha pasión, mucho interés, mucho conocimiento a la realización de este ejercicio de política para que sea fructífero para todos. Con esto de nuevo les agradezco a nuestros oradores hoy por tomarse el tiempo. De nuevo por habernos dado el tiempo para compartir su experiencia y su pasión en el proceso de desarrollo de políticas más emocionante que hemos enfrentado en ICANN desde hace bastante tiempo. Hemos tenido temas desafiantes antes pero este parece ser el más central en los últimos cinco años aproximadamente. Gracias por esta actualización. De nuevo, gracias a Hadia por generar esta serie de seminarios web y por elegir cuidadosamente el tema. Estoy segura de que va a haber una posibilidad para que todos nosotros los actualicemos un poco más. Sin más, quiero

darle la palabra a Hadia. Si quiere abrir este seminario web, tiene la palabra. Alan va a ser el primer orador. Les dejo la palabra a los dos. Si Hadia quiere darnos una bienvenida, lo puede hacer antes de entrar directamente a la presentación que ya veo que está en la pantalla. Luego le doy la palabra a Alan. Gracias a todos por participar. Estamos contentos de tener este seminario web inaugural. Gracias.

HADIA ELMINIAWI:

Muchas gracias, Joanna. Le vamos a dar después la palabra a Alan. Les quiero agradecer a todos por participar de este seminario web.

ALAN GREENBERG:

Aparentemente estaba en silencio. Primera diapositiva, por favor. Ahora sí voy a mencionar la primera parte de esta presentación. Vamos a ver esta primera parte y después ver cómo llegamos a las complejidades de la parte actual. Vamos a ver primero la justificación para el EPDP, cómo llegamos hasta aquí, qué es esta legislación de privacidad y cómo nos afecta, qué ocurrió durante la fase uno del proceso, que tomó un poco más de un año comenzando en octubre del año 2018, si recuerdo bien. Ahora ya pasó un año y medio o dos en el proceso. Ya me perdí un poco en el tiempo en este momento.

Ya estamos muy cerca en teoría de finalizar, a pesar de que, como vamos a ver, es posible que terminemos el EPDP pero todavía no terminamos el trabajo. Son desafíos, retos, muy interesantes. En la parte de abajo van a ver que utilizamos el términos WHOIS para que haya más simplicidad. El término moderno que se utiliza es RDS, que significa servicios de

directorio de registraci3n o RDDs que es el servicio de directorio de datos de registraci3n. Estamos hablando de lo mismo de todos modos. WHOIS tambi3n es el nombre de un protocolo pero a la vez es un nombre que describe el servicio y los datos que estamos analizando. Vamos a usar la palabra WHOIS pero se puede intercambiar efectivamente con los otros t3rminos.

WHOIS es una base de datos que nos dice qui3nes son los registratarios de gTLD. Nos cuenta qui3nes son, nos dicen su identidad, c3mo contactarlos. En la mayor3a de los casos, esta informaci3n puede estar enmascarada por un servicio de proxy. Uno puede pagar aproximadamente un d3lar por mes y pedirle al registrador que no revele ning3n tipo de informaci3n. Este es un servicio que se ofrece desde hace muchos a3os. Hay algunas personas que lo usan, otras no. Tal como ha estado el WHOIS hasta ahora era requerido por contrato con los registratarios y con los registros, es decir, estaban obligados a dar esta informaci3n, y los primeros acuerdos de ICANN con el gobierno de Estados Unidos, que ya expiraron, ped3an que se apoye el WHOIS como protocolo en la base de datos. La divulgaci3n p3blica de informaci3n de personas naturales, y ahora entramos en palabras que quiz3 son nuevas para algunos de ustedes, dentro de la legislaci3n de privacidad nos referimos a personas naturales, que son personas, y a personas legales que son empresas. si bien la palabra personas se usa, a pesar de que est3 modificada por natural o legal, en realidad se trata de informaci3n personal o informaci3n que simplemente es sobre un entidad legal que en muchos casos no est3 protegida por la legislaci3n de privacidad.

Si miran esas dos declaraciones van a ver que están en conflicto una con la otra. No se puede pedir que toda la información sobre el WHOIS sea mostrable, incluida la información de contacto, el nombre, el número, direcciones, números de teléfono y a la vez proteger la información que está asociada con estas personas naturales. Este es el problema que enfrentamos.

La legislación sobre privacidad está vigente en muchas jurisdicciones desde hace mucho tiempo. En general, protege, como dije, a las personas naturales. Les voy a decir por qué estoy usando palabras un poco vagas. Porque no se protege a las personas legales. Si se trata de una empresa, no protege la información. ¿Qué ocurre por ejemplo si en la empresa ustedes utilizan el nombre alan.greenberg@gmail.com como uno de los contactos? Esa información de repente es información personal. ¿Qué ocurre si la empresa se llama Alan Greenberg Incorporated? ¿Eso es una persona? No queda claro. En algunas jurisdicciones se dice que esa es información personal. Es mi nombre. Otras jurisdicciones dicen: "Usted puso su nombre personal en el nombre de una empresa y por lo tanto, en ese contexto, no está protegido". Esto varía dependiendo de la jurisdicción y es interpretado de manera diferente por distintos tribunales. Hay mucha vaguedad en general.

Como dije, hemos visto legislación sobre privacidad en muchas jurisdicciones durante mucho tiempo. Para ser directo, esto ha sido ignorado por ICANN en buena medida. Algunos de nuestros registradores y registros que están sujetos a esto lo tomaron más en serio y ha habido algunas disposiciones que les han permitido distintas

cosas pero en líneas generales no era el foco principal de ICANN. ¿Qué es lo que diferente ahora? La legislación actual en Europa es el GDPR, la regulación general sobre protección de datos. Lo que es diferente del GDPR es que hay multas muy importantes que están vinculadas a este incumplimiento. ¿Qué significa "significativo" para mí? Puede ser hasta 4% del ingreso bruto. No la ganancia sino el ingreso bruto. También hay disposiciones que pueden indicar que uno deje de operar si está cometiendo una violación suficiente.

Las penalidades son amplias. En líneas generales, a uno no le aplican la penalidad máxima por una violación. Las empresas, como los registradores, no tienen un gran margen. Hay un porcentaje de las ventas brutas que podrían borrar toda la ganancia. De repente se convirtió en algo muy importante. El GDPR es complejo y muy técnico. Para aquellos de ustedes que pueden leer la legislación, está disponible en Internet. Son muchas páginas. Cuando uno llega a ese documento, va a encontrarse inmerso en terminología. Si uno no es experto en privacidad de datos privados, se va a confundir un poco.

Está el concepto de los controladores, que en términos simples son aquellos que establecen las reglas pero es mucho más que eso. Si tenemos una relación comercial con alguien, el hecho de que a uno lo perciben como estar en control, incluso si no lo está, podría convertirse en un controlador. Luego están los que realizan los procesos, los que llevan adelante lo que hacen otras entidades. Dentro de la ICANN y de los datos del WHOIS, quién es el controlador no queda claro. Se puede tener un argumento para decir que ICANN fija las reglas y por lo tanto ICANN es el controlador. También se puede decir que el registrador es el

controlador o que hay control conjunto, que es algo más técnico. También se puede argumentar que hay controladores individuales. De hecho, para cada dato, dependiendo de cómo se utilice, puede haber distintos controladores para esos mismos datos. Es un tema un poco complicado.

Hay que tener objetivos para procesar datos. Si yo les pido a ustedes el número de teléfono, tengo que tener una razón para pedirlo. No debería estar pidiendo información que no necesito para realizar lo que yo les estoy pidiendo que realicen. Si ustedes me dan información, la tengo que mantener privada. Algunas informaciones que ustedes me dan solamente podrían tener un significado si las hacemos públicas y obviamente ustedes me están dando permiso para hacerlas públicas. Si no, no estarían en contacto conmigo por ese uso en particular. Otras informaciones que ustedes pueden esperar que yo las tenga en privado, pero que se las puedo revelar a alguien, si es que tienen unas razones que sean lo suficientemente fundadas. Yo tengo que equilibrar la necesidad de privacidad con la necesidad de esa persona de acceder a los datos.

En estos días del coronavirus hay discusiones muy interesantes respecto de si se puede violar la privacidad en nombre de mejorar la salud pública. ¿Esta es una razón suficiente para vulnerar la seguridad privada? Se han tomado decisiones en cuanto a cuánto se valora la privacidad por encima de la seguridad pública. No es un tema fácil y no es algo que necesariamente sea constante todo el tiempo.

Debido a las penalidades, las sanciones que existen, aquellos que son potencialmente responsables claramente tienen una razón para ser muy conservadores. No quieren tomar ningún riesgo. Aquellos que quieren datos y las razones por las cuales uno puede querer datos para proteger la propiedad intelectual pueden ser varias. Si alguien registra un nombre de dominio y lo enmascara como la empresa o lo enmascara como una persona, usted podría tener la necesidad de saber por qué se enmascara. Si estamos haciendo trabajo de ciberseguridad y la gente registra nombres de dominio específicamente para la pesca o para el phishing o respecto de otras cuestiones de ciberseguridad, puede resultar responsable. Si alguien robó un nombre de dominio y lo está utilizando, las personas de ciberseguridad pueden enfrentarlo y decirle que alguien robó ese nombre. Por eso pueden tener que llegar a conectarse.

Todo esto entró en vigencia alrededor de mayo de 2018. Miremos ahora a ICANN. Tenemos el plazo de mayo de 2018 y no estamos listos. Todavía en nuestros libros tenemos políticas que dicen que los registros y registradores deben publicar toda la información que tienen. Los registros y registradores van a ser responsables potencialmente, ICANN incluido, de grandes multas si no siguen las reglas. Las políticas de la ICANN normalmente están establecidas por procesos de desarrollo de políticas que denominamos PDP. Los PDP son procesos de múltiples partes interesadas donde distintas personas de la comunidad, incluyendo At-Large, pueden debatir los temas y tratar de encontrar un punto común en el que puedan estar de acuerdo.

Estamos ahora en una situación en la que no hubo tiempo para poder establecer una política formal. La gente de repente era responsable ante ciertas multas porque no pudimos cambiar las reglas. Por suerte, hay una disposición en nuestro contrato que dice que la junta directiva puede establecer políticas en situaciones urgentes y esto se consideró urgente. Solamente se puede establecer esta política durante un año. La presunción cuando escribimos estas cláusulas contractuales hace muchos años era que durante un año íbamos fácilmente a poder tener una política nueva. La realidad es que el PDP es muy poco probable que tenga una política en un año. Es casi imposible. Podemos desarrollarla pero no será posible implementarla.

En nuestros contratos, los contratos que ICANN tiene con registros y registradores, existe un contrato base donde hay ciertos apéndices y adendas que se llaman especificaciones. Un contrato puede tener 10 o 15 especificaciones para dar los datos de cierta parte de la relación contractual. La junta adoptó una especificación temporaria que se agrega a todos los contratos pero es temporaria, es por un año. Esta es la fuente de este nombre tan confuso, especificación temporaria. Es una parte del contrato pero se puede hacer humo en un año. Siguiente diapositiva.

Tenemos una pregunta. La pregunta es la siguiente. ¿Por qué se estableció la especificación temporaria para remplazar al WHOIS? Vamos a colocar la pregunta en la pantalla.

JOANNA KULESZA:

¿Pueden ver el quiz en la pantalla?

ALAN GREENBERG: No, no. Por favor, pasemos a la diapositiva anterior. Creo que el personal va a tener que hacer su magia para que el quiz aparezca en la pantalla y lo podamos ver todos. Se suponía que eso era lo que tenía que pasar. Muy bien. Tenemos dos preguntas que apuntan a la diapositiva número uno. ¿Por qué se estableció la especificación temporaria? 1. Para remplazar al WHOIS. 2. Porque la especificación no podría ser permanente. 3. Porque la junta directiva no tenía nada mejor que hacer. 4. Porque las reglas actuales del WHOIS podrían ser potencialmente ilegales. 5. Todas las anteriores. Ahora sí, pueden colocar su respuesta. La pregunta para el personal es la siguiente. ¿Cuánto tiempo damos para que se puedan responder estas preguntas?

CLAUDIA RUIZ: Ya voy a ingresar. Un momento, por favor.

JOANNA KULESZA: ¿Alguien pudo enviar? Hay dos preguntas y solamente respondimos una.

CHERYL LANGDON-ORR: Perdón pero hay dos preguntas y hay uno de mis iconos que no funciona. Yo quería responder la segunda pregunta.

ALAN GREENBERG: Perdón. Yo ni siquiera sabía que había un icono que decía: "Enviar". Perdón. ¿Podemos poner nuevamente en pantalla el quiz?

CLAUDIA RUIZ: Perdón. El problema es que ya se hizo el quiz como una continuación. Mientras tanto, lo que puedo hacer es adaptarlo para ver si se puede modificar pero ahora va a continuar si lo coloco en pantalla.

ALAN GREENBERG: ¿Lo podemos adaptar para la próxima vez que haya que colocarlo en pantalla?

CLAUDIA RUIZ: Tenemos cuatro diapositivas más así que voy a hacer mi mejor esfuerzo para hacerlo rápidamente.

ALAN GREENBERG: Vamos a volver a este quiz luego. Siguiendo diapositiva. Muy bien. Ahora estamos en el punto en el cual la especificación temporaria ya fue puesta en vigencia. Tenemos un periodo por delante y sabemos que tenemos aproximadamente un año durante el cual podemos mejorar algunas cuestiones. Como dije anteriormente, establecer una política en un año es un tanto complejo dentro de la ICANN pero solamente tenemos un año. Se estableció un PDP expeditivo que tenía diferentes reglas para poder proceder a una velocidad mayor. Los PDP habituales de la ICANN, todo el mundo que haya participado o que quiera participar lo puede hacer. En los PDP iniciales, hace muchos años, la gente que podía participar era muy limitada. Todo se limitaba al consejo de la GNSO por las características de sus miembros pero hace unos años hay

otra apertura para que más gente pueda participar. Esto cambió y entonces se puede tener participación de todas las partes de la ICANN que quieran participar pero una parte muy restringida de personas dependiendo del grupo al que uno pertenezca puede seguir participando. La idea es garantizar que haya un equilibrio y que se pueda prolongar el proceso para que todos puedan expresarse. En realidad fue un nuevo proceso. Fue una especie de experimento. Siguiendo diapositiva.

Seguimos avanzando a los resultados de la fase uno. Los resultados de la fase uno se obtuvieron en menos de un año. Logramos ese objetivo. Básicamente, la política resultante fue similar generalmente a lo que decía la especificación temporal pero había muchos cambios que se le hicieron a esa política. La mayor parte de los datos personales fueron omitidos. Eso era lo que estaba en la especificación temporal. Además, al igual que con la especificación temporal, esto les permitía a los registrantes omitir la información sobre las personas legales. Esto fue mantenido en la política del EPDP. El EPDP y el GDPR tienen ciertas limitaciones geográficas que protegen por ejemplo dentro de la Unión Europea. También hay cuestiones territoriales como por ejemplo compañías que están en otros países que también deben protegerse. Básicamente, se realiza esta protección dentro de ciertas regiones geográficas.

La política del EPDP le permite a los registradores y registros no diferenciar las regiones geográficas. La divulgación. Si alguien tiene alguna razón por la cual solicitar datos, esto va a ser altamente descentralizado. Tiene que ir al registrador o al registro y pedir los datos,

esto debe ser así. Como ustedes pueden esperar, los resultados fueron muy variables en este sentido. Siguiendo diapositiva.

Esta diapositiva nos adentra en la sección que va a abordar Hadia que tiene que ver con el acceso y la divulgación. Hubo mucho debate dentro del EPDP. Hablamos del acceso y de la divulgación. Desde el punto de vista de una persona que quiere acceso a ciertos datos, la cosa era obtener el acceso. Desde el punto de vista de las partes contratadas se hablaba de la divulgación. Son las dos caras de una misma moneda. Literalmente, esto llevó horas de debate discutiendo qué se debería hacer y la sabiduría de los que sabían dijo que teníamos que abordar ambas cuestiones. Ahora hablamos del acceso y de la divulgación.

Los terceros pueden tener una necesidad legítima de acceder a los datos que han sido omitidos. Estos pueden ser datos personales o no personales. La experiencia con el modelo descentralizado que surgió de la especificación temporal y de la política inicial fue que esto no era satisfactorio. Hubo ciertos rechazos, algunas solicitudes que se consideraron como no razonables. Hubo otras que fueron totalmente ignoradas y que alguien hizo una solicitud y nunca le respondieron o la respuesta venía tres meses después.

La situación era lo suficientemente extraña que tampoco teníamos autoridades de protección de la ley en Europa, es decir, aquellos que tenían que estar al tanto de las leyes de protección de datos. Cuando tenían algún reclamo sobre alguna otra cuestión, tenían que acceder a la información del WHOIS. Después, cuando iban al registrador o al registro, les decían: "No. No les vamos a dar esa información". Entonces

entramos en un círculo vicioso, en una situación perversa donde algunas partes contratadas eran mucho más rígidas al momento de proteger la privacidad ante estas solicitudes. La cuestión es que la cosa no funcionó muy bien. El desafío concreto fue cómo implementar un sistema que permitiera a la gente, a los usuarios legítimos acceder a los datos pero, al mismo tiempo, que protegiera la privacidad que se le debe al titular de los datos individuales. Ahora tenemos otro quiz, otra pregunta. Vamos a pedirle al personal si es que estamos listos para el primer quiz y para el segundo quiz también. ¿Podríamos volver a la diapositiva número ocho, el primer quiz que hicimos?

CLAUDIA RUIZ:

Perdón. Lo puedo agregar. Me lo salteé.

ALAN GREENBERG:

Vamos a hacer este quiz primero y luego vamos a pasar al anterior. La pregunta dice así: "¿Por qué el equipo del EPDP para la especificación temporal para los datos de registración de gTLD fue establecido? ¿Por qué tenemos este equipo del EPDP? 1. Para remplazar la especificación temporal con una política formal. 2. Para crear una política de RDS que cumpla con las necesidades de las partes contratadas. 3. Para crear una política que cumpla con las necesidades de los usuarios. 4. Todas las anteriores". Tienen que elegir una respuesta y hacer clic en el icono "Enviar".

La mayoría respondió remplazar la especificación temporal. En realidad, la respuesta correcta es "Todas las anteriores". Lo que tratamos de

hacer es claramente remplazar a la especificación temporal. También que esto resulte en una política que cumpla con las necesidades de las partes contratadas y que las proteja y, al mismo tiempo, garantizar que los usuarios legítimos puedan tener acceso a los datos según lo establece el GDPR. Tenemos la primera pregunta que mostramos del quiz. ¿Estamos listos? Podemos volver luego.

CLAUDIA RUIZ:

La vamos a poner en pantalla en la próxima oportunidad.

ALAN GREENBERG:

Muy bien. Siguiendo diapositiva. Ahora llegamos a la fase dos del EPDP. Aquí hablamos de la creación o el diseño de un sistema estandarizado de acceso y divulgación, el SSAD. El concepto aquí es tener una ubicación única para enviar las solicitudes. Si se requieren datos que fueron omitidos que no son públicos, hay que ir a un lugar específico para solicitar esos datos. Es una forma estandarizada de hacer solicitudes. Habrá una revisión. Les estoy dando parte de los resultados y parte del diseño porque durante el debate hubo muchas otras variaciones a todo esto. Básicamente es lo que tuvimos como conclusión. Había luego les va a contar los detalles con más exactitud pero básicamente estas son las generalidades de lo que obtuvimos como resultado. Habría una revisión estandarizada y un proceso de respuesta. Cuando uno envía una solicitud, se le va a verificar que esté completa y si no, va a ser rechazada hasta que esté finalizada. Si ahora se hace una solicitud, sabemos quién lo hace y cuándo lo hizo.

Vamos a tener que determinar quién es uno porque en primer lugar es necesario entender a quién se le están dando los datos. Este es un requisito según el GDPR pero lo más importante es sobre la base de quién es uno puede haber ciertas características que tengamos que tener en cuenta. Pueden hacer esto por una cuestión de ciberseguridad, pueden ser agencias de cumplimiento de la ley, pueden tener un propósito específico. Sobre la base de quién es uno, se puede recibir un tratamiento diferente. No se les va a dar acceso automático a cualquier dato. Hay algunos datos donde sí se tiene acceso automático pero son datos muy restringidos. Sobre la base de quién es uno, se puede actuar.

La financiación es algo crucial. Cómo vamos a pagar todo esto. Claramente tiene que haber cierto costo que tengan que pagar los usuarios y también algún otro costo que abonen otras partes. El precio puede variar. Podemos darles a las agencias de cumplimiento de la ley un precio distinto al que le damos a por ejemplo las agencias de propiedad intelectual, que lo hacen por una razón meramente comercial. El financiamiento y las tasas que se cobren van a ser algo muy importante dentro del proceso. Es muy difícil hablar de precios cuando no se tiene idea de lo que va a costar. En este punto exactamente no tenemos ninguna idea en absoluto de lo que va a costar. Verdaderamente, este es un desafío. Siguiendo diapositiva.

En este punto creemos que va a ser un sistema centralizado, administrado por la ICANN. El SSAD solo aceptará solicitudes de solicitantes acreditados. Autenticará y validará las consultas. En este punto, el SSAC va a enviar la consulta a las partes contratadas que será un registrador o registro para que la revise y para que posiblemente la

apruebe y responda. La respuesta va a provenir directamente del registrador, lo cual va a evitar transpolar el flujo de datos. Por ejemplo, que un dato que está en una localidad vaya a los Estados Unidos y de allí al usuario. Básicamente esto va a hacerse a través del registrador. Si hay datos personales, y recuerden, nosotros en muchos casos omitimos información sobre las personas jurídicas, puede no haber información personal. Puede ser que los datos tengan que ser liberados inmediatamente porque la legislación no pide que estos se oculten. Básicamente lo que tenemos que hacer es una prueba de equilibrio. Tenemos que evaluar la razón que tiene quien solicita los datos y tenemos que compararlo con las necesidades que tienen los individuos que están involucrados en relación a la privacidad. Muchos creen que esto lo tiene que hacer un ser humano. Es decir, tiene que haber alguien encargado de esto en lugar de hacerlo de manera automática.

Actualmente tenemos una pequeña cantidad de casos en los cuales creemos que el SSAD en sí puede determinar si no hay ninguna cuestión por la cual no se pueda liberar el dato y entonces se le envía al registrador o al registro la pauta para que lo haga. Se hace todo en un registro. Cuando se liberan estos datos, esto va a estar en un registro y también lo que después vamos a tener son estadísticas de rendimiento para que todo el mundo sepa cómo está funcionando.

Me parece que la diapositiva que sigue tiene que ver con otra pregunta. Es la siguiente. "¿Quién puede enviar solicitudes al SSAD?" Las posibles respuestas son: 1. Todos aquellos que conozcan el URL correcto. 2. Solo aquellos que están acreditados formalmente. 3. Solo los que puedan pagar el costo. 4. Ninguno de los anteriores.

La gran mayoría señala que son solamente aquellos que están acreditados. Realmente esa es la respuesta correcta. "Solo aquellos que pueden pagarlo" se podría aplicar pero también puede haber gente que no tenga que pagar. Entonces la respuesta general es la que se dio. Pasemos al siguiente quiz. Vamos a preguntarle al staff si ha hecho lo que tenía que haber hecho hace 30 minutos. Si no estamos listos, entonces avanzamos con la presentación. Es la pregunta sobre la diapositiva número ocho la que quiero ver en pantalla. Entonces lo dejamos de lado. Le vamos a dar la palabra a Hadia y luego, al final, vamos a seguirlo. Hadia, le doy la palabra. Adelante, por favor. ¿Podemos bajar por favor esa pregunta que está en pantalla y volver a la diapositiva 16, por favor? No vamos a hacer el quiz ahora. Le vamos a dar la palabra a usted, Hadia. Vamos a volver al final. Pido disculpas. Nuestro plan era parar antes de cada quiz y preguntarles si había algún comentario y me olvidé. Pido disculpas. Espero que no tengan muchos comentarios.

HADIA ELMINIAWI:

Está bien, Alan. No hay problema. Para resumir, después de que un usuario haya sido acreditado, el solicitante puede presentar un pedido para que se muestren los datos públicos de registro. El pedido típicamente va a contener información como el nombre de dominio vinculado con esa solicitud, algunos elementos de datos que el solicitante pide también y el derecho legal vinculado. Además, si se trata de un pedido urgente, por ejemplo, se lo puede agregar. El gestor central, que es la entidad estandarizada, es el que va a ser el responsable de recibir el pedido y a veces puede tomar alguna decisión.

Después de que el manager del portal central recibe la solicitud, se continúa con la información brindada.

CLAUDIA RUIZ:

Hadia, disculpe que la interrumpa. Los intérpretes están teniendo problemas para escucharla. Quizá si puede acercarse al micrófono.

HADIA ELMINIAMI:

Al haber recibido el pedido de divulgación hay que tener un sistema estandarizado de divulgación y allí se confirma que toda la información requerida y brindada se haga de una forma automatizada. Si la información requerida está incompleta, el sistema estandarizado para acceso/divulgación va a dar una oportunidad para que el solicitante pueda modificar y presentar nuevamente la solicitud. Una vez que esté completada la información, el SSAD va a responder con una respuesta automatizada y va a mirar el pedido. Si es uno de los casos de uso que se consideran automatizables, el sistema estandarizado de acceso/divulgación va a tomar una decisión respecto de si se divulga o no. Si la decisión es divulgar los datos, el manager del portal central va a pedirle a la parte contratante correspondiente que se divulguen los datos del solicitante.

Tenemos solamente dos casos posibles para automatización. El primero tiene que ver con los pedidos de las autoridades de aplicación de la ley en la jurisdicción correspondiente y el otro tiene que ver con las respuestas a un problema de resolución de disputas para que haya aclaración de los solicitantes. Si bien esto todavía no es completamente

cierto, lo hemos estado discutiendo bastante pero eso es lo que tenemos por el momento. Si el pedido no es uno de los casos acordados, que en este momento hay solo dos casos, el manager del portal central va a mandar la solicitud a la parte contratada, como dijo antes Alan, y puede hacer una recomendación a la parte contratada respecto de si se debe divulgar o no. Esa parte contratada puede seguir la recomendación realizada por ese portal central pero si no lo hace, debe informar a ese gestor del portal central sobre la razón por la cual la recomendación no se siguió, para que el sistema pueda mejorar en cuanto a las recomendaciones futuras.

Con el tiempo, se espera que el sistema mejore la toma de decisiones y las recomendaciones que realizan este manager del portal central y también las partes contratadas. Los datos disponibles en relación con la cantidad de solicitudes y los tipos se supone que tienen que mejorar el acuerdo de nivel de servicio. Por lo tanto, un mecanismo que permita que evolucione el sistema sin que haya necesidad de hacer un PDP cada vez y sin que se agregue una mejora, es esencial y es algo que es requerido. De nuevo, hasta ahora no hemos acordado ningún mecanismo. Hemos estado discutiéndolo mucho y espero que podamos llegar a algo en ese sentido. Las partes contratadas pueden requerir un portal central para automatizar algunas partes de estos pedidos de divulgación o todas ellas.

Tenemos ahora el quiz. "¿Quién es responsable de tomar la decisión de divulgar los datos al solicitante dentro del SSAD?" Si podemos ver las respuestas. Ahora están en pantalla. 1. El SSAD en sí mismo, los registros y registradores. Cuando decimos el SSAD, es el central gateway

manager, que es el responsable de tomar la decisión con ciertos casos automatizados y por recibir el pedido. 2. Los registros y registradores. No hay ninguna decisión necesaria. 3. Todos. 4. Ninguno. Esas son todas las opciones.

La respuesta correcta es "Todas las anteriores". Hay dos casos. Si es un caso automatizado, el gateway central va a responder y va a tomar la decisión. Si no lo es, el registro o registrador correspondiente es el que lo va a hacer. A veces no hay ningunos datos personales para divulgar. Si vamos a la siguiente diapositiva, por favor.

La siguiente diapositiva es sobre la acreditación. Antes dijimos que para poder utilizar el sistema hay que poder ser un usuario acreditado. ¿Qué significa la acreditación? La acreditación es una acción administrativa a través de la cual la autoridad de acreditación declara que un usuario tiene derecho a acceder al sistema. La autoridad de acreditación va a confirmar y verificar la identidad del usuario. Le va a enviar al solicitante alguna credencial como un usuario y una contraseña, y esas credenciales identificadas en el usuario pueden utilizarse por el central gateway manager o para hacer validación. La autoridad de acreditación también le da al usuario ciertas credenciales y esas credenciales o afirmaciones firmadas tienen información como el objetivo del pedido y la base legal del pedido. Las credenciales de identidad tienen una afirmación que está firmada. Va a haber solo una acreditación de parte de ICANN y la ICANN puede trabajar por ciertos proveedores que van a verificar la identidad del solicitante y firmar la afirmación.

La acreditación sola no asegura la divulgación de los datos. Solamente permite el uso. La decisión de divulgar o no se realiza entre el central gateway manager y las partes contratadas. Se toma la decisión de la divulgación y se confirma la identidad y la base legal para el pedido. De todos modos, cada solicitud es examinada en mérito propio por parte del central gateway manager o la parte contratada. La autoridad de acreditación puede revocar la acreditación del usuario. Este caso puede incluir el hecho de que no exista más la posibilidad de acreditación, que se haga un uso indebido del sistema por parte del usuario y la autoridad de acreditación también va a ser auditada. Es decir, todas las actividades de acreditación como las solicitudes de acreditación, la información sobre los fundamentos para acreditar o verificar la identidad, todo esto va a ser registrado por la autoridad de acreditación y por los proveedores de identidad. Si pudiésemos tener la siguiente diapositiva, por favor, que es un quiz.

“¿Cuál es el rol de la acreditación en SSAD? 1. Extraer dinero de los solicitantes. 2. Asegurar que conocemos a quien está haciendo el pedido. 3. Ayudar a entender por qué el solicitante necesita todos los datos. 4. Todo lo anterior. 5. Ninguna de las anteriores”. Los resultados, por favor. Extraer dinero de los solicitantes. Ese no es un objetivo pero eso está sucediendo porque la acreditación no es gratuita. Asegurarnos de que nosotros sabemos quién está haciendo el pedido, sí. Confirmar la identidad del solicitante y recuerden que la acreditación también da afirmaciones respecto de los objetivos del solicitante. Todo tiene que ver con entender por qué el solicitante necesita los datos. La respuesta correcta es: “Todas las anteriores”.

ALAN GREENBERG: El uso de “extraer” fue a propósito allí.

HADIA ELMINIAWI: Obviamente, no se trata de extraer pero hay un cargo, o sea que sí, eso es así. En cuanto al tiempo de respuesta, cuando un solicitante hace un pedido al sistema, la información que se brinda incluye un tipo de respuesta como por ejemplo si es un pedido urgente que es una prioridad uno o si es un UDRP o un URS. En ese caso es prioridad dos. Todas las demás solicitudes son prioridad tres. Un pedido urgente de acuerdo con lo que tenemos en el informe actualmente, esa respuesta se recibe en un día hábil. Quiere decir que si uno presenta una solicitud el viernes a la tarde, puede tener la respuesta el lunes.

Los pedidos urgentes dependen de las circunstancias donde hay un riesgo de la vida, daño físico una infraestructura crítica online u offline. Un ejemplo es un banco o un sistema de electricidad, algo que se le parezca. De nuevo, estas solicitudes urgentes requieren respuestas urgentes. De nuevo, una vez que el sistema está operativo, tenemos datos que nos dicen más sobre la cantidad de pedidos y de tipos. Es decir, cuántos son urgentes, cuántos son prioridad dos o prioridad tres. Esto puede ayudarnos a determinar los acuerdos de nivel de servicio mínimos. De nuevo, esta es una de las razones por las cuales el sistema podrá mejorar. Los mecanismos pueden permitir un modelo híbrido para mejorar pero es esencial tener un sistema eficiente.

No podemos tener un acuerdo de nivel de servicio significativo ahora porque no tenemos los datos que nos permitirían que esto sea así. También hemos podido únicamente automatizar algunos casos pero después de que el sistema entró en operación sería bastante obvio que hay algunos otros casos que hay que automatizar. Esto es útil no solamente para los solicitantes porque ellos están recibiendo sus respuestas rápidamente. La respuesta no tiene que ser que sí. Puede ser un no pero también resulta útil para las partes contratadas.

Pedimos disculpas los intérpretes pero tenemos mal audio de Hadia.

Una vez que terminemos el tema de las personas naturales versus las legales, los operadores pueden diferenciar entre una persona legal y natural. También hemos concluido que hablamos de la factibilidad. Hay implementación de los costos y la diferenciación entre personas legales y naturales. Ejemplos de organizaciones. Los riesgos que puede haber también con los registrarios de acuerdo con la organización de la ICANN. Este es un breve cuestionario para tener los aportes, la factibilidad y el costo de la diferenciación entre personas legales y naturales, y el informe puede ser compartido en mayo de 2020 pero de nuevo el equipo del EPDP no ha podido llegar a ningún tipo de consenso en este sentido y la recomendación es consultar a la GNSO respecto de cómo se supone que va a haber hallazgos en este tema. Hay que consultar a la GNSO sobre los pasos próximos en este sentido. No hemos llegado a esta conclusión. La GNSO debe tener esto en cuenta.

El otro tema que es muy importante, y todavía no hay ninguna conclusión en relación con eso, es la precisión. No se define la palabra

pero la ley de protección de datos de 2018 define "impreciso" como algo que no es correcto. El GDPR no establece bien los datos. De acuerdo a la información, el GDPR incluye una obligación clara de tomar medidas para corregir los datos que no son correctos. Vemos esto como un tema importante que está dentro del alcance. La GNSO tiende a la precisión dentro del alcance pero debido a las limitaciones de tiempo el equipo del EPDP no se va a ocupar de esto. Se generará un equipo para explorar un poco más el tema en relación con la precisión y un sistema de registro de la precisión. Estos son dos temas importantes. Todavía no ha cerrado la primera parte. El segundo y el tercero ya están cerrados. Siguiendo diapositiva, por favor.

"¿Qué protege el GDPR? 1. Todo almacenado en una computadora. 2. Todo dato enviado a las grandes corporaciones. 3. Cualquier tipo de datos personales como por ejemplo nombre, dirección y edad. 4. Datos asociados con las registraciones de nombres de dominio". Bien. Todo dato personal como por ejemplo nombre, dirección o edad. Todo tipo de dato como por ejemplo número de seguridad social, datos biométricos, nombre, dirección. Básicamente todo tipo de información que pueda utilizarse para identificar o rastrear la identidad de un individuo, eso es lo que protege el GDPR. Gracias. Voy a detenerme aquí. Ahora voy a darle la palabra a Alan.

ALAN GREENBERG:

Esperamos poder volver al primer quiz. Quiero que mi quiz aparezca. Muy bien. Ahí está. "¿Por qué se estableció la especificación temporal para remplazar al WHOIS? 1. Porque las especificaciones no pueden ser

permanentes. 2. Porque la junta directiva no tiene nada mejor que hacer. 3. Porque las reglas actuales sobre el WHOIS son potencialmente ilegales. 4 Todas las antes mencionadas". La respuesta correcta es que las reglas actuales sobre WHOIS pueden ser potencialmente ilegales.

Antes de iniciar el debate quiero que volvamos a la diapositiva número 24. Voy a señalar lo siguiente. Todo esto tiene que ver con el punto de vista del ALAC referido al debate que tuvimos y a otros puntos de vista que son sumamente importantes. Cómo respondemos a los resultados del EPDP va a depender mucho de hasta qué punto el mecanismo esté desarrollado. Si pensamos que va a funcionar o no, cuál va a ser el resultado final y cuál es la exactitud que va a tener, y también el tema de las personas jurídicas y de las personas físicas. Creo que el ALAC puede aceptar estos resultados y, como mencionó Hadia en este punto, la recomendación en el informe preliminar es que no hagamos nada en relación a los últimos dos puntos y que regresemos esto a la GNSO para que continúe trabajando. Es decir, tenemos que esperar a ver qué dice el informe final y cuál es la respuesta a todo esto. Ahora sí, les doy la palabra en caso de que tengan preguntas o comentarios. No han levantado la mano. Joanna, adelante, por favor.

JOANNA KULESZA:

Gracias, Hadia. Gracias, Alan, por la presentación. Estuve haciendo un seguimiento en el chat. Creo que hay algunas preguntas de Rick Lane con respecto a una diapositiva en particular que tiene que ver con la información brindada. No sé si quieren que yo la lea o quieren que lo

repita para poder abrir el debate o si ya fueron respondidas oportunamente.

ALAN GREENBERG: Yo no estaba mirando el chat así que no las respondí. No sé si Hadia o alguien más lo ha hecho.

HADIA ELMINIAWI: No. Yo tampoco leía las preguntas del chat. Joanna, si quiere las puede leer.

JOANNA KULESZA: Las voy a leer. Rick, si quiere tomar la palabra, lo puede hacer. La primera pregunta es una solicitud para poder definir las agencias de cumplimiento de la ley en las correspondientes localidades o regiones. Holly indica que este es un tema en sí. También hay otra pregunta por parte de Rick que tiene que ver con quién toma la decisión de aceptar los datos personales y quién es el que toma la decisión final. Voy a darles la palabra a ustedes para que respondan. Veo que hay más preguntas por parte de Rick. Adelante, Alan.

ALAN GREENBERG: El cumplimiento de la ley. Si uno es por ejemplo un registrador en Alemania, entonces tiene una obligación legal de responder a ciertas solicitudes que provienen de las agencias de cumplimiento de la ley de Alemania. Si uno tiene una solicitud de alguien más en otra parte de la Unión Europea, es posible que exista un cierto acuerdo y que haya que

responder pero si uno obtiene un pedido de alguien en los Estados Unidos, realmente no hay ninguna garantía de que las agencias de cumplimiento de la ley puedan demandarle a usted que dé una respuesta porque no está en los Estados Unidos. En realidad, las agencias de cumplimiento de la ley de Estados Unidos van a tener que contactarse con las agencias de cumplimiento de la ley en Alemania para poder obtener la información.

La cosa se puede complicar mucho. Para darle un punto de vista más simple, no siempre se va a tener una obligación de responder a una autoridad de cumplimiento de la ley según la jurisdicción. A eso nos referimos con el cumplimiento. Si la agencia de cumplimiento de la ley está en su jurisdicción, entonces va a tener ciertos derechos que otras agencias de cumplimiento de la ley probablemente no vayan a tener.

ORADOR DESCONOCIDO: ¿Entonces quiere decir que GoDaddy y Verisign no van a tener que responder?

ALAN GREENBERG: Si tienen una oficina en Europa, entonces probablemente sí tengan que responder si se hace un enfoque a ese grupo pero eso ya pasa mi nivel de conocimiento. No lo sé. En general, se puede establecer para cualquier registro qué agencia de cumplimiento de la ley debe responder obligatoriamente. Todo fue enumerado correctamente. Hay mucha documentación al respecto. En cuanto a quién toma la decisión, esa es una pregunta bastante compleja. En general, el responsable del

tratamiento de los datos es el que toma la decisión. Recuerdo que al comienzo dije que no se sabe quiénes son los responsables en cada caso y si la ICANN es el responsable del tratamiento de datos y esa decisión va a depender de una legislación de privacidad, que la ICANN tiene que implementar, entonces va a haber ciertas cuestiones donde se debata si los registros y registradores tienen que ser los responsables. También va a haber otras situaciones en las cuales estos también pueden ser multados o tener ciertas sanciones que cumplir. Si tuviéramos esa respuesta con facilidad, no estaríamos dedicando tanto tiempo a este debate. Se supone que la ICANN era el responsable y que la ICANN podía tomar la decisión y que no iba a ser un tema de responsabilidad en relación a los registros y registradores.

RICK LANE: Mi pregunta tenía que ver con quiénes toman la decisión a un nivel general. Todos los que toman las decisiones pueden estar en conflicto o tomar otra decisión.

ALAN GREENBERG: No, lo puedo responder. La decisión va a depender del pedido. Puede ser que se cuestione, que se haga una solicitud o no. Es decir, para algunas clases de datos, aquí está la gran pregunta. Si se sabe que no son datos personales, se pueden liberar. Punto. No hay ninguna limitación en esto. Si por ejemplo hay datos cuyo tipo de solicitud, como mencionó Hadia, ya se decidió que se podía automatizar, el SSAC va a tomar la decisión. En el caso general, va a ser la parte contratada. Todo lo anterior no se

aplica sino que cualquier solicitud puede ser respondida por cualquiera de estas tres partes.

HADIA ELMINIAWI:

Si me permite, yo quiero agregar algo más. Por favor, tengan en cuenta que cuando hablamos de cumplimiento de la ley desde el punto de vista de la jurisdicción, estamos hablando de esta divulgación automática. Recuerden que tenemos en el sistema estandarizado de acceso y divulgación dos cuestiones. Se analiza la solicitud primero. Si es una solicitud pero se ha automatizado, esto quiere decir que este caso puede ser respondido de manera automática. En este caso el gestor del portal central va a responder la solicitud y va a tomar la decisión. La decisión puede ser un sí o un no. Si la decisión es un sí, entonces va a pedir a la parte contratada que libere los datos. Hasta ahora tenemos solo dos casos de uso en este sentido. Esto no quiere decir que otras agencias de cumplimiento de la ley de otras jurisdicciones no vayan a hacer una solicitud. Pueden hacer una solicitud pero probablemente no sea una automatizada. Cuando el portal central analiza la solicitud y ve que no es una solicitud de la misma jurisdicción o equivalente a la agencia de cumplimiento de la ley, dirige esta consulta a la parte contratada y la parte contratada la analiza y decide si va a divulgar o no la información.

Una cuestión importante a tener en cuenta es la siguiente. Las agencias de cumplimiento de la ley, las entidades gubernamentales también tienen ciertas autoridades de acreditación pero esta autoridad de acreditación será responsable de acreditar a estas autoridades

gubernamentales para que puedan acceder al sistema estandarizado de acceso y divulgación.

También veo una pregunta que dice si las partes contratadas pueden hacer registraciones con las personas naturales. Bueno, lo que sucede es que no se está diferenciando entre personas jurídicas y personas humanas. Este es uno de los problemas que surgen en cuanto al campo de organización. No hay un campo de organización todavía. Incluso si hay datos en estos campos no se garantiza que el registratario pueda identificarse a sí mismo correctamente. Podríamos decir que lo que sucede es que muchas de las registraciones son de personas humanas aunque no lo sean. Esta es una de las cuestiones que surgen, una de las cuestiones por las cuales se hace esta clasificación.

JOANNA KULESZA: Gracias, Hadia. Voy a tratar de responder todas las preguntas. Tenemos otras preguntas de Rick. Tenemos a Joan, que ha levantado la mano. No sé si quisiera tomar la palabra.

ALAN GREENBERG: Démosle la palabra a Joan primero y después respondemos a Rick.

JOANNA KULESZA: Joan, adelante, por favor. También tenemos algunas otras preguntas por parte de Rick. Si no las quiere leer, las puedo leer yo. Joan, adelante, por favor.

JOAN KATAMBI: Muchísimas gracias. Gracias, Hadia, por la excelente presentación. También quiero agradecer al equipo que está detrás, Alfredo y Joanna. Tengo una pregunta para Hadia. Tomando en cuenta el tiempo de respuesta, ¿importa si se reciben por ejemplo mil consultas? Si se obtiene una sola consulta, ¿se va a responder? Gracias.

HADIA ELMINIAMI: Gracias por la pregunta. Por lo general, el tiempo de respuesta es un día. Esto no tiene que ver con el número de solicitudes o consultas. Independientemente del número, hay algunas que son urgentes y según el acuerdo de nivel de servicio van a tener que responder dentro del plazo de un día laboral. Para algunas solicitudes, un día es demasiado tiempo. Este periodo de 24 horas es más adecuado pero la respuesta de las partes contratadas es que todavía no saben el nivel de solicitudes que van a recibir o cuáles van a ser urgentes y cuáles no. Por el momento se van a atener a este periodo de 24 horas porque no saben el volumen que van a recibir. Por el momento es un día hábil, independientemente de la cantidad de solicitudes que se presenten.

ALAN GREENBERG: Si me permite, quiero agregar algo. Las solicitudes urgentes tienen que ver con cuestiones que amenazan la vida o cuestiones graves. No esperamos que haya una gran cantidad de ese tipo de consultas. El acuerdo de nivel de servicios establece algunas cuestiones y se van a graduar estas consultas. La idea no es tener una demanda absoluta sino un cierto promedio. En realidad, esto es bastante flexible por el momento. Se entiende bien que va a haber que analizar qué es lo que

sucede y cuáles son las adaptaciones que se van a hacer pero no se puede tener ningún plazo porque después no hay manera de poder tomar una acción contra aquellos registradores que no responden, por ejemplo. Joanna tiene la palabra.

JOANNA KULESZA: Muchas gracias por las respuestas. Veo que hay más preguntas que agradecen compartir estas respuestas.

ALAN GREENBERG: Solamente nos quedan 10 minutos. Vamos a ser muy breves.

JOANNA KULESZA: Yo voy a tratar de identificar y leer las preguntas de Rick. Entiendo que muchas son comentarios pero voy a tratar de resumirlas. La primera dice así: "Si todos los anteriormente mencionados toman las decisiones en el acceso, ¿quién tiene acceso al proveedor de identidad y quién toma la última decisión al respecto? ¿Eso no sería una violación del GDPR?" La segunda pregunta creo que es un poco más sencilla. "¿Cuál es el plazo para completar?" La tercera es: "¿Quién tiene acceso a la información?" Perdón, ya la respondimos. Básicamente esas serían las tres preguntas. Quién tiene acceso a la información sobre el proveedor de identidad y cuál es el plazo para que esto se complete. Quizá ustedes también quieran responder algo en el chat.

ALAN GREENBERG: Creo que la pregunta sobre la decisión tiene que ver con el solicitante, no con el proveedor de identidad.

JOANNA KULESZA: Eso es lo que dice la pregunta en el chat.

ALAN GREENBERG: Si el solicitante es una persona física y tenemos información sobre personas físicas, eso va a estar protegido por el GDPR y la legislación de registración. Hay una serie de legislaciones que dicen quién puede obtener datos del SSAD y también de dónde se pueden obtener y quiénes pueden obtener información o datos del RDS. Tenemos algunos debates sobre hasta qué punto se pueden hacer públicos estos datos. Si un solicitante, ya sea una persona humana o una persona jurídica, ¿deberíamos liberar esta información o tendría que seguir siendo privada? Claramente vamos a hacer muchos informes. Muchos van a ser públicos y otros no. La privacidad del solicitante también es un tema que vamos a tener que considerar durante la implementación de todo esto.

En cuanto al plazo, es una muy buena pregunta. No sabemos cómo va a funcionar el sistema. Seguramente tenga que haber cierto diseño. Estamos analizando varias de las funciones y estamos trabajando con la ICANN. La ICANN y otros organismos también hacen este tipo de funciones. Seguramente vamos a hacer algunas adaptaciones. No reinventar todo de nuevo pero básicamente establecer el proceso de acreditación para determinar quién va a poder acreditar. Por ejemplo aquellos letrados que tengan que ver con la propiedad intelectual o

profesionales de marcas comerciales o profesionales de ciberseguridad. Y luego crear un proceso mediante el cual podamos establecer, en el caso de ciberseguridad, cuáles son las credenciales. Es decir, no todo el mundo va a poder decir que es un agente de ciberseguridad. Esto lleva tiempo así que supongo que si podemos implementar todo en un año sería glorioso pero no creo que vaya a ser así. No sabemos cuál va a ser el plazo todavía, para ser honestos.

HADIA ELMINIAWI:

Quiero decir una cosa más en relación con el proveedor de identidad. Se ha dicho que la autoridad de acreditación y el proveedor de identidad todos podrían estar logueados pero eso se debe divulgar cuando la divulgación es necesaria y hay una obligación legal de la autoridad de acreditación o el proveedor de identidad. Estoy leyendo la pregunta que dice si hay acceso a la identificación del proveedor de identidad. Yo no estoy muy segura de qué quiere decir esa pregunta pero se trata de información registrada. Si estamos hablando de esa información registrada, solamente se divulga en relación con una obligación legal para cuestiones de auditoría.

JOANNA KULESZA:

Gracias a Hadia y a Alan. Escuché que alguien estaba tratando de hablar. Si hay alguna otra pregunta de la audiencia la podemos tomar. No veo ninguna mano levantada.

ALAN GREENBERG:

Veo una pregunta de GG Levine en la pantalla.

JOANNA KULESZA: Creo que esa es la pregunta que acaba de leer Hadia pero Alan, le doy la palabra.

ALAN GREENBERG: ¿Tenemos alguna cuestión de la seguridad sobre los usuarios? ¿Creemos que la expurgación de los datos nos está afectando? Creo que esa es la pregunta que se hace. La respuesta es que por eso estamos aquí. Creemos que hay importantes temas para los usuarios no registratarios. Varios miles de millones de usuarios no registratarios comparados con los cientos de miles de registratarios. Para todos ellos, el WHOIS ha estado siendo utilizado en la ciberseguridad, en investigaciones que incluyen cuestiones como los filtros de spam durante mucho tiempo. La imposibilidad de acceder a esa información creemos nosotros ahora que está impactando significativamente en los usuarios. Cada usuario que usa email se ha beneficiado de filtros de spam. Cada persona que usa un navegador web tiene el beneficio de distintas características de seguridad que están en el navegador y que utilizan información que se recolecta en los sitios web y también en nombres de dominio donde se dice si uno puede confiar en esos sitios o si hay alguna vulnerabilidad. Sí, nosotros creemos que los usuarios finales están y van a estar siendo incluso más impactados por la ciberseguridad. En particular está el hecho de que el GDPR ha sido sobreimplementado en la expurgación de muchas informaciones que no deben ser expurgadas. Esto hace que a las partes contratadas les resulte más difícil la implementación pero el impacto es grande sin duda.

JOANNA KULESZA:

Gracias, Alan. Creo que es un excelente comentario en este webinar que nos vuelve a llevar al desarrollo de políticas. Gracias por la pregunta. Quisiera saber si nuestros oradores tienen algún comentario final. Tenemos tres minutos antes de la finalización de esta llamada. Si no es así, les voy a agradecer a todos por haber participado. Quiero agradecer especialmente a nuestros presentadores de hoy. Les agradezco por haberse tomado el tiempo para ayudar a la comunidad a entender dónde estamos y de dónde proviene este proceso. En representación de Alfredo y de mí misma les quiero agradecer y decirles que esto ha sido muy útil. Siempre estamos abiertos a preguntas y a comentarios. Le quiero agradecer a Hadia por establecer este webinar y por planear los próximos. Estén atentos a los anuncios que va a haber pronto, donde se van a incluir los procedimientos posteriores, uso indebido del DNS, geopolítica, etc. Le quiero agradecer especialmente por haber hecho que este webinar sea interactivo. Esta es una iniciativa donde tenemos las preguntas en el medio de la presentación. Fueron muy buenas para asegurar que podamos seguir la información que se está presentando. Con esto entonces les agradecemos a todos. Les agradecemos a nuestros intérpretes y a nuestro personal. Esperamos poder verlos en el próximo seminario web que va a generar nuestro equipo de At-Large. Muchas gracias a todos. Esta reunión finaliza aquí.

[FIN DE LA TRANSCRIPCIÓN]