ICANN79 | Foro de la comunidad – Sesión 2 del plenario de At-Large: creación de confianza en el Internet a través de la verificación de registratarios
Miércoles, 6 de marzo de 2024 – 4:15 a 5:30 SJU

MICHELLE DESMYTER: Esta sesión va a comenzar. Empiecen la grabación. Hola y bienvenidos a la reunión plenaria número dos de At-Large, la sesión de construir confianza a través de la verificación de registratarios. Soy Michelle DeSmyter y soy la coordinadora de participación para esta sesión. Por favor, tengan en cuenta que esta sesión está siendo grabada y se rige por las normas de conducta de la ICANN.

Durante esta sesión, las preguntas o comentarios serán enviados al chat y se leerán en voz alta si se formulan de la manera como lo he indicado en el chat. Por favor, levanten la mano en Zoom cuando deseen hacer una intervención. Los participantes in situ activarán sus micrófonos antes de hablar. Por favor, digan su nombre y el idioma en que hablarán si van a hablar un idioma que no es inglés. Hay interpretación en francés, inglés y español. Les damos la palabra a Michael Palage y Avri Doria.

MICHAEL PALAGE: Hola. Soy Michael Palage y soy el comoderador de esta sesión, junto con Avri Doria. La forma en como haremos esto es que vamos a hacer de esta sesión algo muy interactivo entre los participantes que están en línea y los que están in situ. Yo voy a coordinar las actividades de aquellos que están en el salón y Avri va a estar coordinando las actividades y las conversaciones a través del pod de preguntas y respuestas y el chat en Zoom.

La forma en como hemos desglosado esta sesión es con dos paneles. El primer panel será para discutir el tema de la confianza. Tenemos distinguidos expositores. La segunda parte de la sesión será una ronda de la mesa donde los participantes podrán dar un informe breve sobre cómo los diferentes operadores de registros independientes están viendo la parte de la verificación de los registratarios y cómo están pidiendo otras credenciales para mejorar esa verificación. Esta es la hoja de ruta que vamos a seguir. Por temas de tiempo y consideración a los expositores le doy la palabra a Finn Petersen, el director ICT en temas de gobierno digital. Finn, adelante.

FINN PETERSEN: Gracias. Si me permiten, ¿puedo ver mi diapositiva? Gracias por invitarme. Aparte de mi trabajo en la agencia danesa también soy presidente de dos grupos de trabajo en Europa. Uno sobre medidas de seguridad digital para infraestructura digital y servicios. También soy presidente del área de trabajo de WHOIS. Voy a hablar sobre el Artículo 28.

Aquí hay un vistazo breve de lo más importante en cuanto a esta directiva de WHOIS y el Artículo 28. Les exhorto a todos a que lo lean. Yo he tratado de resumirlo. Aquí vemos en esta solicitud los registros y las entidades que dan los servicios de registros de nombres de dominio. Estamos hablando de los registradores, revendedores y proveedores privados.

Existen ciertos requerimientos. Ahí están los requerimientos que aplican según sea el caso, si son entidades privadas dentro de la Unión Europea o no. Aquí se ha dado un cuestionamiento, si se pueden recopilar los datos aun cuando no se haga uso de ellos. Lo correcto es recopilarlos para que sea seguro y poder tener una Internet segura y estable.

En esta directiva NIS2 también se ha especificado que hay que recopilar el nombre de dominio y también la fecha de registración, el nombre del registratario, el número de teléfono, un correo electrónico. Si no se ha hecho esto, se necesita la dirección y el teléfono de la persona encargada. Estos datos tienen que ser precisos, tienen que estar al día y tienen que estar verificadas. La información entonces tiene que ser precisa, completa y debe estar verificada. También hay una obligación de publicar en el sitio web de WHOIS la información que sea información de carácter no personal. También publicar información para personas jurídicas o entidades legales. Dichas personas jurídicas aun cuando contienen un nombre legal. Por ejemplo, si yo tengo una empresa que está registrada con un nombre con personería jurídica, ese nombre tiene que estar registrado

también, no solamente el nombre comercial. Hay una obligación de dar acceso a los datos de WHOIS para aquellas personas que piden acceso por temas legales y a solicitudes que sean debidamente sustanciadas.

Esto es una norma dentro de las directivas que luego se traducen a leyes nacionales en todos los países de la Unión Europea. Tienen un tiempo de siete meses y medio para implementarlo. Tienen libertad para implementarlo y para poner otras normas o requerimientos adicionales a estos, que son los básicos de la normativa. Hay una recomendación de que deben cooperar e intercambiar la información con la comisión para efectos de borradores o algunas normas de implementación.

En este sentido han creado un flujo de trabajo y eso es lo que se ha creado en WHOIS. El propósito es redactar las guías o lineamientos para el Artículo 28 en la norma NIS2 se pueda implementar con un enfoque armonizado y que se utilicen dichas cláusulas en la normativa que se implementa a nivel nacional. La idea es tener, como dije, un enfoque armonizado. Sabemos que hay muchas entidades bajo esta obligación. La idea es que no tengan condiciones muy distintas dependiendo de cuáles sean los estados miembros o jurisdicciones que la utilicen.

Hemos creado en este flujo de trabajo dos grupos de tareas. Hay uno que va a trabajar en el tema de verificación. Ellos redactarán los borradores de las guías para establecer qué se debe hacer para verificar los datos que ya existen y cuáles son los datos que se deben

pedir para verificar. Los datos deben ser precisos, deben estar actualizados y deben ser verificados. Emitiremos guías en cuanto a esto también. Sabemos que es mucho trabajo tener que revisar los datos ya existentes y que ya fueron recopilados pero es un requerimiento bajo la norma NIS2.

El otro grupo de trabajo se va a especializar en el legítimo acceso. Es decir, determinar quiénes son las personas que pueden acceder a esta información o pedir acceso a esta información. Esto será cuando se dé respuesta a estas solicitudes que pidan información sobre la información que es considerada como privada o restringida dentro de lo que es WHOIS.

Estos datos deben ser entregados o suministrados en un plazo de 72 horas según la ley. También está definido cómo se debe manejar una solicitud urgente. En esta comunidad hay muchas guías que van a ser revisadas por los estados miembros y la idea es llegar a una guía que sea armonizada o que sea consensuada por todos. Pueden leer el texto y quizá pueden darse diferentes interpretaciones por parte de los diferentes estados miembros y todavía estar dentro del alcance de la norma. Hay que observar los detalles.

Lo ideal sería que existieran los mismos detalles en cada estado miembro que está implementando esto de forma tal que se sigan las guías. Si emitimos estas guías, la idea es que todos los estados miembros lleguen a un acuerdo sobre las guías y cómo se aplicarán estas regulaciones. La armonización es clave en todo esto.

Eso con referencia al Artículo 28 de la norma. Hay otros criterios, por supuesto, que afectan a los proveedores de DNS, CDN, [ISP]. Eso tiene que ver con las medidas de seguridad. Aquí aplicarán nuevas reglas por parte de la Comisión Europea en la llamada Ley de Implementación. He sido responsable de dar mi aportación técnica en cuanto a ese documento. No necesariamente esto se traduce a leyes nacionales pero sí se traduce a reglamentos que deben seguir los operadores que están operando dentro del alcance de esta reglamentación.

MICHAEL PALAGE: Finn tiene que regresar al GAC y a trabajar en el borrador del comunicado. Si hay preguntas, por favor, pónganlas en el chat y con gusto las pondremos en línea para todos.

FINN PETERSEN: Lamento no estar allí. Creo que esto es mucho más interesante que la redacción del borrador del comunicado, pero me pagan por estar allí.

MICHAEL PALAGE: Gracias. Quisiera presentar a Karla McKenna. Es directora de gestión y responsable de normas en la Fundación GLEIF. Ha pasado a ser una de mis organizaciones internacionales favoritas. Para los colegas que me conocen, a menudo la menciono. Le paso la palabra a Karla para que explique la historia de GLEIF, lo que hacen y para que potencialmente brinde un mapa de ruta para ver lo que está tratando de hacer la comunidad de nombres.

KARLA MCKENNA: Es un placer estar aquí y poder presentarles estos temas hoy. Siguiente, por favor. Para confirmar el temario, va a ser las generalidades del sistema global LEI, algunos de los temas que comentó Michael, que se vinculan con la crisis financieras de 2009 y después cómo LEI forma la base de lo que se ha venido haciendo en los últimos años. Siguiente.

El sistema global LEI fue denominado así por los líderes del G20 para crear un identificador de entidades globales que identifique de manera unívoca las partes de las transacciones financieras. No solo se pueden identificar las instituciones financieras. Se le puede asignar a un ambiente muy amplio y a una lista amplia de personas jurídicas que existen a nivel internacional que participan en operaciones financieras. Inclusive para el departamento de tesorería de una sociedad anónima.

La fundación LEI fue creada bajo el G20 y con los antecedentes de que está vinculada a la crisis financiera del 2008 para que los reguladores y las empresas y el sector privado puedan comprender aquellos que tienen responsabilidad legal de distintos roles en distintas operaciones financieras y los responsables de la transparencia, la exposición, supervisión y demás.

GLEIF se creó bajo supervisión regulatoria. GLEIF es el operador responsable de la integridad del sistema global LEI. Tenemos una red de asociados que validan que las personas jurídicas existan y la información sobre las mismas que luego se transporta a GLEIF y se

publica sin restricción bajo Creative Commons y sin contratos de licencia de uso en el repositorio global LEI que llamamos sistema global LEI.

Vamos a ver estadísticas de GLEIF. Tenemos la junta. Somos una organización sin fines de lucro. Tenemos más de 2.5 millones de LEI emitidos a la fecha. Es importante tener en cuenta que el identificador de personas jurídicas es una norma de la ISO. Los reguladores lo llaman cuando tratan de verificar lo que había sucedido. Quieren poder comunicarse a través de las fronteras en algunos casos dentro de la misma jurisdicción entre organismos gubernamentales con una identificación común porque no existía nada a nivel internacional. Allí empecé a involucrarme en GLEIF porque fui parte del desarrollo en la ISO para elaborar la norma de LEI como norma internacional de la ISO. Siguiente, por favor.

Los asociados que tenemos en el sistema global de LEI que validan la existencia de las personas jurídicas y cierta información sobre ellos, eso llevó a considerar que tenemos un cimiento muy sólido con los LEI para poder pensar en cómo poder hacer que sea más útil además de ser un código vinculado con datos estándar de referencia.

Empezamos a pensar qué podríamos hacer para poder hacerlo relevante desde la perspectiva de identificación digital. Pensamos que lo que teníamos constituía una base para brindar lo que llamamos el LEI verificable, que es un equivalente digital usando LEI. Lo que ofrecemos aquí es la posibilidad de tener una identidad de la organización para que una persona o cosa pueda probar que tiene la

capacidad de representación de la organización a través del LEI externamente o inclusive dentro de los límites de las organizaciones, porque algunas son muy grandes y no todos conocen a todos, los cargos de cada uno ni sus funciones.

Así empezamos el camino para poder crear el LEI verificable y credenciales organizacionales que pudieran comprobar con seguridad, capacidad de verificación y certeza. Lo que ofrecemos aquí, lo que elaboramos para el LEI verificable es la arquitectura de cero confianza para la identidad organizacional a través de credenciales organizacionales. Lo que queremos poder hacer aquí es respaldar el movimiento a fin de modificar el comportamiento de los usuarios que reciben documentos, archivos y otros elementos, otras informaciones, inclusive cuando realizan operaciones financieras o de otro carácter para, por ejemplo, actuar entre consumidores, entre empresas.

Queremos ser parte de ese movimiento para ofrecer funciones dentro de los LEI con requisitos de multifirmas. También las claves criptográficas para mantener seguridad en el uso de las VLEI en cuanto a la identidad de la organización en primer lugar. Siguiente, por favor. Me olvido de las divisiones de sección.

Lo que creamos aquí es la posibilidad de que una organización vaya a un emisor de un VLEI a través de un programa estructurado. Calificamos todos los años para poder darle a la organización una credencial con su LEI y permitir que la organización solicite credenciales adicionales que llamamos de rol. Eso representa la conexión entre las organizaciones, personas y los roles que

desempeñan dentro o en representación de las organizaciones poniendo los mundos digitales y real uno al lado del otro representando la organización por el LEI y pudiendo identificar a la persona mediante credenciales de identificación y el rol.

Lo hemos hecho en dos variables. Una pensando sobre cómo hacerlo desde el punto de vista del papel oficial y con los casos de uso y las conversaciones que tuvimos con la gente de la industria y también aquellos en las áreas tecnológicas que respaldan los LEI pensamos utilizar las credenciales para poder apoyar a los roles funcionales o definidos para cosas de uso en particular y poder ampliar el valor de los VLEI. Siguiente.

Les voy a llevar a través de la cadena de confianza de los VLEI. Nos establecimos como fundación para los VLEI y mencioné brevemente antes que estas credenciales van cambiando. Con estas nuevas tecnologías y protocolos que utilizamos podemos crear una cadena de confianza, no solamente para el que emite las credenciales sino para que sean los cimientos para la verificación criptográfica de las credenciales a posteriori cuando se las utiliza y se las presenta. GLEIF califica a los emisores de VLEI y cuando emiten las credenciales a las organizaciones se utiliza la cadena para poder vincular las credenciales de las organizaciones con emisores calificados de VLEI y todas las credenciales de roles que comentamos para poder criptográficamente vincularlas con la organización que emitió la credencial. También con la organización que las emita para ver cuál es el emisor calificado. Esta cadena de verificación bajo el principio de cero confianza puede

permitir que el verificador o quien reciba la credencial verifique todo el camino de vuelta para ver que el LEI existe y está en el sistema global de LEI.

Vamos a ver cómo se utilizan. En el uso de las VLEI he tratado de dar un par de ejemplos sobre cómo se puede utilizar para las empresas, sector público y personas físicas estas verificaciones en tres áreas distintas. Hay casos de uso para poder respaldar las funciones en recursos humanos, incorporación de empleados, autorizaciones, representación fuera de la empresa, aparición de clientes, formularios, taxonomías, informes. Hay un gran potencial en poder utilizar los VLEI para poder firmar documentos a medida que pasan por la cadena de abastecimiento física hasta el área de finanzas. Vemos una gran oportunidad para poder acceder a los servicios públicos así como para poder utilizar los VLEI.

Un par de ejemplos. Vamos a ver la siguiente diapositiva. Uno de los casos de uso que quería mostrarles son las firmas digitales. Esto es algo en lo que estamos trabajando muy activamente. La firma digital y el caso de uso correspondiente es muy sólido para las presentaciones obligatorias y voluntarias.

Comenzando a la izquierda, la empresa que informa presenta un archivo a un regulador, firma con el LEI. La entidad que lo recibe puede verificar la validez criptográfica de la credencial y la firma, y también la organización que toma el LEI y lo compara con una amplia lista viendo que esta sea una organización sobre la que quería hacer la averiguación el organismo. Es una especie de mostrador de

verificación. La entidad que la recibe puede aceptar el archivo en base a la verificación.

En la siguiente diapositiva tenemos un piloto en el que estamos trabajando activamente que se presenta ante la Autoridad de Banca Europea. Tenemos casos de informe de sector privado al público y la EBA tiene 17 bancos. Hay un trabajo publicado recientemente que está buscando opiniones de las instituciones hasta fines de marzo. Después de un piloto exitoso la EBA va a anunciar la decisión de su uso para la información y la implementación para el total de 600 bancos que tienen que informar la EBA, remplazando los 27 informes de las autoridades nacionales de las cuales ahora la EBA recibe sus informes. Esto cubriría la identificación, autenticación, autorización, seguridad y gestión de los usuarios a cargo de presentar estos marcos a la EBA.

Una diapositiva más antes de cerrar. Quería mostrarles que una gran parte del ecosistema y la infraestructura de los VLEI consiste en el marco de gobernanza. Algo en lo que participé y de lo cual soy responsable. 24 documentos en total que cubren todo, desde la emisión y la revocación de credenciales, la rotación de las claves, los requisitos para el emisor de los VLEI calificados que se centra en ellos, en los usuarios que cumplan con todos los requisitos operativos y gubernamentales para el sistema de VLEI. Muchos de estos requisitos se incluyen en el software desarrollado y por los proveedores que quieren utilizar este identificador.

MICHAEL PALAGE: Gracias, Karla. Quisiera ahora pasarle la palabra al siguiente orador, que también es la co-coordinadora y comoderadora de la sesión de hoy, la señora Avri Doria, amiga de muchos en la comunidad, incluido yo. Si podemos ver las diapositivas de Avri. Avri tiene la palabra.

AVRI DORIA: Gracias, Michael. Gracias por la introducción. Básicamente voy a tratar de hablar sobre por qué es tan difícil encontrar un espacio de solución para las identidades digitales. Volviendo al tema de la ICANN y nuestro deber, que es confiar en un modelo de múltiples partes interesadas. He sido parte de varios procesos. El más reciente, el de RDAP, SSAD, entre otros.

Se determinó que el problema era que no encontrábamos un punto de consenso entre los diferentes actores con diferentes políticas. No teníamos una claridad en cuanto a cómo lidiar con la parte de la información de seguridad y la parte de la privacidad. Es ahí donde hay diferentes instituciones que necesitan cierta protección o cualquier organización.

Tenemos que seguir trabajando en los consensos y llegar a estos consensos y ver cuál sería el impacto de estas evaluaciones y de lo que hagamos en los derechos humanos. No había una arquitectura o un conjunto de protocolos que pudiese hacer eso. Colectivamente no pensamos que había una solución digital para hacer esto pero la mayoría lo vimos y pensamos que no había una solución. Eso no ayuda

mucho a crear confianza. Es un poco preocupante cuando no se puede encontrar una solución en un determinado punto.

Hoy escuché una conversación sobre el número de registratarios y estamos pensando en esto. Estamos viendo el problema y muchas de las soluciones que se sugirieron no son viables técnicamente. Utilizar unas cuantas herramientas posiblemente no sea algo posible en este momento pero la pregunta es: ¿Es posible utilizar quizá una combinación de herramientas y políticas para obtener los resultados ahora y que mejoren a lo largo del tiempo? ¿Hay un rol que ICANN pueda asumir para encontrar una vía, un camino hacia una solución?

Viendo estas preguntas cruciales empecé a ver los temas de protocolo, empecé a hablar con diferentes personas y llegamos a crear esta hermosa galaxia de soluciones de identificación digital. Al verlo, vi muchos protocolos y realmente hay una riqueza, una abundancia de opciones. Hay protocolos para firmas electrónicas. Hay protocolos de autenticaciones. Hay protocolos para identificar a entidades jurídicas. Obviamente hay temas con el lenguaje de seguridad que utilizan algunos, entre otras muchas cosas. Todo cabe dentro de esta galaxia pero no existía una sola herramienta que resolviera todo el problema en su totalidad.

En una presentación impresionante vi que había muchos ccTLD que utilizaban una combinación de estas herramientas que daban como resultado la funcionalidad básica que se necesita. Recomiendo que vean esa presentación más adelante, si no la han visto. Hay ciertas

brechas y en función de las posibles soluciones tengo preguntas en cuanto a la escalabilidad.

Viendo esta galaxia de soluciones de identificaciones digitales pienso que son buenas pero no necesariamente pueden coexistir o funcionar conjuntamente. Por ejemplo, mi fascinación más reciente es con ITF, WHIMSE, que son los entornos para múltiples entidades. Se trata de una combinación de las herramientas y las arquitecturas. Quizá pueda ofrecer una ruta de solución. Empecé a recopilar información.

Empecé a recopilar información sobre muchos de los protocolos que existen en esta galaxia y estoy tratando de entender cuáles son los que usan y con qué propósito para entender mejor el poder combinado que tienen y saber qué tanto puede abarcar la solución, siempre teniendo en cuenta los temas de privacidad y derechos humanos. Este trabajo está abierto para que sea comentado, que se hagan observaciones y para mejorarlo, por supuesto.

Esta es la parte de la solución técnica y eso deja dos áreas más en las que hay que trabajar. Creo que una solución técnica es viable. La otra parte de este panel va a dar una mirada más profunda al tema. Vamos a hablar de los temas que tienen que ver con la protección de datos y derechos humanos. Gracias.

MICHAEL PALAGE: Gracias, Avri. Ahora vamos a ver el segundo panel. Este será el de la mesa redonda donde básicamente vamos a dar presentaciones de tres a cuatro minutos por varios operadores de TLD que han implementado

la verificación de registratarios en diferentes niveles. El primero será Lucas Prêtre, que es ingeniero de telecomunicaciones en OFCOM, la Oficina Federal de Comunicaciones, y nos va a hablar sobre el gTLD .SWISS.

LUCAS PRÊTRE: Gracias, Michael. Gracias por este espacio. Gracias por darme la oportunidad de presentarle a la comunidad lo que hacemos para la verificación de registratarios en el gTLD .SWISS. Siguiente diapositiva, por favor. Los nombres de dominio de .SWISS están destinados específicamente a entidades ubicadas en Suiza. En general las que están en el registro comercial suizo pero hay ciertas excepciones. Los criterios están definidos en la ley sobre dominios de Internet. La solicitud del registratario contiene lo que llamamos eID, el número de identificación de la empresa o persona jurídica en Suiza. Esta identificación nos permite consultar nuestra base de datos a nivel nacional para ver lo que hay en los registros.

Podemos tener varios resultados primero. Que el número de la identificación de la empresa no existe o que se escribió mal. Cuando vemos esos casos, que no se encuentra, se rechaza la solicitud con un código de rechazo. Cuando se encuentra, entonces tenemos que esa entidad y su formulario legal se muestran en nuestra herramienta de evaluación que tiene diversos campos. Esta herramienta ha sido desarrollada específicamente para .SWISS. Es bastante automatizada y hace el trabajo del registro de la empresa.

Algunos formularios son específicos para Suiza y son diferentes a los de otros países. No todos los campos que están en el formulario es obligatorio que estén en el registro comercial suizo pero aquí voy a ver el artículo 55 de la ley que habla sobre la elegibilidad de las solicitudes. Hacemos una evaluación del lazo que existe entre el solicitante y el dominio que se está solicitando.

Primero determinamos si es un producto o un proyecto. Siguiente diapositiva. Tenemos cuatro tipos de relaciones o de lazos o nexos entre el solicitante y el dominio. Por ejemplo, si es una marca registrada, se basa en el nombre, el nombre de la empresa. Es un reconocimiento general si es un producto o un proyecto dentro de esa empresa. Si no, entonces podemos ver que quizá no hay un nexo entre el dominio solicitado y el solicitante o si es un término genérico. Esas son las causas taxativas para rechazar esas solicitudes.

Como ven en la diapositiva tenemos un cambio en cuanto a la elegibilidad. En abril de 2024 abrimos los criterios de elegibilidad para personas naturales. Estas personas naturales o físicas tienen que dar su número de identificación personal. En el caso de Suiza es el número de seguro social de la persona física. Creo que se me ha acabado el tiempo. Perdónenme. No sé si quieren escuchar sobre el RDAP, el protocolo de acceso a los datos de registración.

MICHAEL PALAGE: Creo que es importante. Te doy 30 segundos.

LUCAS PRÊTRE: Siguiente diapositiva, por favor. Nuestro socio en la parte técnica ha hecho una búsqueda del RDAP de un nombre de dominio. Si es otro cliente se puede ver este número de identificación. Ese número de identificación es público y se puede ver en la base de datos. Con esto me detengo.

MICHAEL PALAGE: Muy bien. Gracias. Las diapositivas están disponibles en línea. Los exhorto a que lo vean, especialmente la parte de RDAP. La siguiente expositora es la señora Lewis, que está en la Junta de Farmacias. Es experta en el tema de salud digital. Tiene la palabra.

NIAMH LEWIS: Muy bien. Voy a hablar rápido porque estoy en otra conferencia ahora mismo. Creo que no voy a durar ni los cuatro minutos que tengo asignados. Queríamos comenzar con que NBAP opera el TLD .PHARMACY. La Asociación Nacional de Juntas de Farmacia es una organización sin fines de lucro cuyos miembros son los 50 reguladores estaduales de la práctica de farmacia en Estados Unidos.

Nuestros miembros son los reguladores gubernamentales y también de farmacia y otras jurisdicciones, incluidas 10 provincias canadienses. NABP hace mucho tiempo que fue creada. .PHARMACY es solo parte de lo que hacemos. Somos una organización cuyo papel consiste en proteger la salud pública. Tenemos más de 180 personas, más de 12 farmacéuticos en nuestra nómina, abogados, incluida yo y otro tipo de personal. Hay una serie de programas que ofrecemos para proteger la

salud pública. Para todos los farmacéuticos matriculados en Estados Unidos, la NABP crea un examen, un programa de acreditación, inspecciones, transferencias también de los farmacéuticos que se mudan de estado. Siguiente, por favor.

¿Qué hacemos con .PHARMACY? El TLD está disponible para los comerciantes de productos de la salud y aquellos que están vinculados con la salud, que han obtenido la acreditación de comerciantes de productos de salud de NABP o de otro programa reconocido o que esté en acreditación. El TLD también está disponible para los reguladores de farmacia.

La acreditación de comerciantes de productos de la salud es un programa global. Hay criterios de elegibilidad. Hay que cumplir con normas tales como si tienen la matrícula correcta, si cumplen con la ley. Hay normas de privacidad. Eso es fundamentalmente. Si revisamos solicitudes en Estados Unidos o fuera de los Estados Unidos colaboramos con los reguladores, MHRA en Reino Unido, NAPRA en Canadá.

Los revisores incluyen abogados, farmacéuticos y abogados farmacéuticos. ¿Cómo se utiliza el .PHARMACY? ¿Cómo lo usan los terceros? Michael dijo que quizá había gente interesada. La idea es que sea un sello a prueba de fraude. Hay muchos sellos en Estados Unidos. Algunos no están acreditados por la asociación cuyo sello tienen en sus pantallas. Nosotros somos a prueba de fraudes. Se requieren ciertas acreditaciones, una de las cuales es la nuestra. Hay otras reconocidas por si quieren hacer publicidad en distintas plataformas tales como

Google, Bing, TikTok y otras. También Visa y MasterCard reconocen nuestra acreditación. Tienen ciertos requisitos en sus programas para gente que tienen farmacias donde no se ve físicamente la tarjeta de crédito y requieren dado el riesgo acreditaciones u otras cosas. La nuestra es una acreditación reconocida pero no es la única. Hay más de 600 nombres de dominio de .PHARMACY registrados.

MICHAEL PALAGE: Muchas gracias. La liberamos para que vaya a la otra conferencia. Nuestro próximo orador, Craig Schwartz, es el director gerente de los servicios de registros de fTLD.

CRAIG SCHWARTZ: Vamos a hablar de .INSURANCE y .BANK. Está restringido a los bancos minoristas, productores de seguros, reguladores. Dadas estas restricciones los potenciales registratarios son menos. Nuestros dominios bajo gestión son pocos. Sin embargo, no es esta la única métrica de éxito. El 17% de los bancos en Estados Unidos están utilizando activamente su dominio .BANK para los consumidores de su base de clientes.

Como dijo Karla hoy sobre los LEI, el 80% de nuestros registratarios en Estados Unidos ya tienen LEI. Estamos tratando de incorporarlos en nuestro proceso de verificación. Somos uno de los pocos gTLD que hacen prerregistraciones preverificadas y les voy a contar sobre esto en un momento. Lo que hace que esto sea más seguro es que requerimos distintos protocolos y tecnologías para los dominios de

nuestra zona. DNSSEC, encriptamiento de TLS, autenticación de correo electrónico. Tenemos estos requerimientos y monitoreamos su cumplimiento a diario.

Estoy orgulloso de decir que hace 10 años que estamos en operación. Han resultado no positivas las verificaciones que se hicieron. Además de los dominios de segundo nivel hacemos cosas jerárquicamente para los TLD. En 2018 pasamos a ser el primer TLD no-Google añadido a la lista precargada. Si uno tiene el certificado adecuado tiene una resolución en el DNS con conexión HTTPS. Después de nuestro viaje de cinco años con el IETF implementamos lo que llamamos DMAC, que tiene una capa de protección de phishing, spoofing de dominios no existentes. Si alguien quiere saber más de esto pueden acercarse y me preguntan.

Siempre trabajamos con un registro y manualmente aprobamos los registros nuevos para verificar que los datos coincidan con los que verificamos. También que nada se cuele por los rincones. Para la verificación en la cual nos basamos tenemos bases de datos públicas regulatorias y confirmamos la elegibilidad de la organización para la selección de nombres, la dirección de correo electrónico, si están en alguna lista negra en base a la lista del tesoro de los Estados Unidos. También verificamos que el contacto del registratario tenga autorización de la organización para mantener el nombre. La verificación se da previo al registro inicial y anualmente a posteriori, o si hay algún cambio de registro tal como la organización registrataria, el contacto o el correo electrónico.

Solíamos encargarlo a Symantec. Era muy complejo para los registradores y muy caro. En 2017 presentamos un RSEP a la ICANN para crear el DRV o la verificación de registratarios dinámica. Lo venimos haciendo con éxito desde hace cinco años, en gran medida manualmente pero vale la pena pagar por la confianza en estos TLD. La evolución siguiente va a involucrar mayor automatización, LEI posiblemente y AI de ser posible.

MICHAEL PALAGE: Gracias, Craig. Quisiera hacer una pregunta. Alan Greenberg pregunta en el pod de preguntas y respuestas cuál es el costo de los LEI. ¿fTLD tiene un LEI? ¿Cuál es el costo anual?

CRAIG SCHWARTZ: Creo que pagamos 60 u 80 dólares por el LEI a Bloomberg.

MICHAEL PALAGE: Nuestro próximo orador es Tom Keller, miembro de la junta ejecutiva de DENIC tiene la palabra.

THOMAS KELLER: Gracias, Michael. Queremos mostrar lo que hemos tratado de hacer ahora que estamos sujetos al DNS también este año. Unas cuantas palabras sobre DENIC. DENIC es una organización sin fines de lucro basada en Frankfurt, Alemania. Estamos legalmente constituidos y estamos sujetos a las nuevas regulaciones.

Hablamos con nuestros miembros. Pasamos por un proceso para decidir qué era lo que íbamos a hacer y les podemos decir qué es lo que pensamos actualmente. Obviamente la ley todavía no ha sido aprobada. Vamos a esperar a la implementación. Vamos a ver si sería una buena idea o no. Creo que es algo que podemos compartir con ustedes. Siguiente diapositiva.

DENIC tiene casi 18 millones de registros de dominios. Es el segundo TLD más grande del mundo. Tenemos 290 miembros y uno de los records más bajos en vistas a los TLD. Ven que es una operación bastante importante. Tenemos que tener mucho cuidado con lo que hacemos. Tenemos muchos registros que ya están ahí. Eso quiere decir que no son como 500. Es muy complicado para nosotros.

Cuando juntamos creamos el grupo para ver lo que queríamos hacer, primero empezamos por los principios. Dijimos que tiene que ser orientado hacia el futuro. No queremos un proceso donde tendríamos que cambiar en algún momento para hacerlo completamente de nuevo. Tiene que ser algo que sea escalable, flexible y tiene que tener un enfoque basado en riesgo. Eso quiere decir que podemos transferir los dominios pero solamente lidiamos con dominios que están en cumplimiento de la ley. Si algo no se ve bien, no lo procesamos. Nosotros ofrecemos posibilidades de verificación X posts y X under. Estas verificaciones se pueden utilizar inclusive para otros TLD. Es un concepto que hemos estado tratando de implementar. Veremos cómo nos va con eso.

¿Qué es lo que vamos a verificar? Queremos verificar el nombre, la dirección, si existe, si es falso o no, el correo electrónico y el número de teléfono. El proceso genérico que vamos a implementar según lo hemos pensado puede ser una queja o un nuevo registro. Primero es que vemos la parte de sintaxis y que esté completa, la verificación de la completitud. Luego esa es una validación y evaluación del riesgo. Ahí decimos que tenemos todo bien del registratario o si hay algo que te indique que no es buena idea registrar este nombre de dominio. Si es de alto riesgo lo ponemos en cuarentena. No lo vamos a delegar y lo manejamos de manera diferente. Si es de alto riesgo, el dominio se delega y se hace una verificación adicional. Si es de bajo riesgo, no hay verificación adicional necesaria.

¿Quién va a hacer la verificación? Ese fue un debate bien largo. Si teníamos que hacerla nosotros o los miembros. El registrador tiene que hacer la verificación y ejecutarla. Tiene que probar que lo hizo si se le solicita. Aquí tenemos varios métodos de verificación que les permitimos a los miembros para ver cuál se ajusta a su modelo de negocios. Gracias.

MICHAEL PALAGE: Gracias, Tom. Es bueno ver que han dejado que los registradores tengan sus propias soluciones. El siguiente expositor es el Dr. Bruce Tonkin, de .AU.

BRUCE TONKIN: Estos son los requerimientos de .AU. Básicamente dice que los registradores tienen que tener presencia en Australia, que sean ciudadanos australianos o que tengan registrada una empresa en Australia. Puede ser una empresa extranjera que tiene presencia en Australia y está registrada allí. También tenemos, por ejemplo, .AU directo, que solo requiere una presencia australiana. Tenemos COM.AU y NET.AU. Ahí tienen que tener una entidad comercial registrada. ORG.AU debe estar registrada y ser una organización sin fines de lucro. Debe estar registrada como tal en Australia. También tenemos las entidades gubernamentales y educativas. Simplemente se puede verificar contra las bases de datos del gobierno.

Hay que validar la información que da el registrador versus lo que vemos en las bases de datos. Si se ve que no está verificado, estábamos hablando de un identificador, una especie de clave de ese verificador. Nosotros verificamos la información contra la base de datos del gobierno. Se ve si la persona existe o no, y eso es suficiente para hacer el registro.

La mayoría de los registradores en Australia deben verificar que el nombre, la dirección y el número de identificación son reales. La mayoría en Australia utilizan el número de registro gubernamental. Esto es algo que se puede buscar de manera gratuita. Es bastante fiable el dato. Se puede buscar con el nombre de la persona, de la empresa y se compara con la información que le ha dado el registratario. Una vez verificado, se puede registrar el nombre del dominio.

Otra posibilidad es que la persona no tenga un nombre comercial, que sea solamente un ciudadano, una persona física. En ese caso se verifica la licencia de conducir o el pasaporte, algún tipo de identificación personal. El gobierno tiene esta información. El único problema con eso es que cobran por verificar ese dato en una base de datos gubernamental. Si se está utilizando su licencia de conducir, a veces necesitan un segundo nombre, a veces no. Puede ser que la verificación salga mal si no se usa el nombre tal cual como está.

A veces ponen el número de licencia de manera equivocada. A veces le cuesta dinero a ese registratario si se rechaza la verificación porque han ingresado de manera incorrecta su información. Ese es uno de los retos que hemos encontrado. Es una manera válida de presentar una validación de la información.

Los registratarios pueden poner su pasaporte o su licencia de conducir. No hay ningún requerimiento de que quede almacenado ese número en el sistema. Simplemente se va a hacer una corrida de verificación cuando se ingrese en el formulario de validación pero no hay que almacenar esos identificadores. Esa es mi información personal y es como la licencia de conducir.

Tenemos algunos registros dolosos que son pocos. Si alguien registra un nombre o un dominio para cometer algún tipo de delito, si se da el caso es con identidades robadas. Usurpación de identidad. Si encuentran la licencia de una persona y es una licencia válida obviamente va a pasar la validación. Es diferente que si es una tarjeta de crédito donde les van a congelar las transacciones. No encontramos

muchos registros dolosos. Hemos visto que algunas organizaciones a veces no actualizan sus nombres en sus sitios web y los hackean. Eso es todo de mi parte.

MICHAEL PALAGE: Gracias, Bruce. Ahora le voy a dar la palabra a un buen amigo y colega, un colega más joven, Jaromir Talíř, un colega técnico. Jaromir, tienes la palabra. Es de CZ.NIC.

JAROMIR TALÍŘ: Nuestro registro es uno de esos registros donde nos importa mucho la verificación, por lo menos desde los últimos 20 años, por lo menos desde 2006 cuando lanzamos nuestro nuevo sistema de registro. Empezamos con algo sencillo, que era mandar una carta a los registratarios cuando recibíamos datos incorrectos o cuando había información sospechosa. Al no recibir respuesta sobre la carta simplemente borrábamos el dominio.

Por supuesto que no podemos verificar de esta manera toda la zona de países de la comunidad. Ahora lo que tenemos es el Servicio de Identidad Digital. Ellos pueden verificar los datos en el nivel que deseen con los servicios de verificación de las identidades de los ciudadanos. Este sistema de verificación ha sido reconocido por el gobierno y da acceso a los sistemas gubernamentales y es utilizado en toda Europa. De esta manera verificamos los ciudadanos pero también tenemos que verificar, por supuesto, si vienen de otros países o países

extranjeros. Tratamos de unir fuerzas con otros ccTLD y sacamos provecho de la verificación a través del eIDAS.

El año pasado lo que hicimos fue rescribir nuestro sistema de verificación donde introdujimos un portal, un sitio a través del cual las partes pueden seleccionar el método de verificación que quieren que se le aplique. Para futuro estamos buscando una interpretación con los registros en línea. Tenemos el registro de GLEIF para verificar las organizaciones. También somos parte de la billetera europea digital. Esto lo hacemos para verificación de registros pero quizá también la podemos utilizar para otros fines. Esto es para personas que tengan identificaciones digitales. Hay quienes no las tienen todavía. Habría que ver cómo verificar a estas personas que no tienen identificación digital.

Por supuesto, la verificación completa hay que determinar cuándo debe ser obligatoria o voluntaria. Por ejemplo, si es para darles dominios a un precio más económico o darles algún tipo de credencial como dueños o titulares de esos dominios o ver si algún otro tipo de servicio que se les pueda brindar. Eso es todo.

MICHAEL PALAGE: Gracias, Jaromir. Timo es el próximo orador. Es el jefe de desarrollo de .EE. Tiene la palabra. Adelante.

TIMO VÖHMAR: Soy de la Fundación de Internet de Estonia. Somos una organización sin fines de lucro para la gestión del .EE. Tenemos identificación de contactos desde 2010. Trabajamos con el modelo de registro-registrador-registratario, con la obligación de la identificación de los contactos por parte del registrador.

Hemos tenidos dos desafíos. El primero, identificar los contactos extranjeros. Esto no es un problema en Estonia porque tenemos una infraestructura de identificación bien establecida. También cómo permitir que los registradores identifiquen y autentiquen los contactos. Hasta ahora hemos utilizado lo que llamo identificación bancaria de las cavernas. Es decir, si hay una transferencia bancaria que tenga los mismos detalles que la solicitud de un registro de dominio se autentica el contacto. Esta solución puede ser muy onerosa en caso de pagos internacionales desde fuera de la Unión Europea. Siguiente, por favor.

Ahora tenemos una mejor solución para estos problemas. Lo llamamos EUID, porque es mejor eID. Es una compuerta de una lista larga de opciones. Por ejemplo, soluciones gubernamentales de Estonia, Letonia, Suecia, Bélgica, España, pero también soluciones privadas como my ID o ID de bancos de Nordics.

Con esto nuestros registradores no necesitan intervenir de manera directa, ahorrando mucho tiempo y problemas en la gestión de estos contratos e intervenciones directas. Para casos en que los contactos no tienen acceso a EUID le damos una identificación propia. Nos hemos asociado con un proveedor de servicio pero hay una serie de

proveedores de este servicio de todo el mundo con la clientela de bancos, instituciones financieras, operaciones específicas. Saben lo que hacen y son muy buenos.

Utilizamos la FIDO ID, que es una norma abierta para el manejo de datos creada por la FIDO Alliance que consiste en nombres grandes en el negocio de Internet. Amazon, Google, Visa, MasterCard, lo que se les ocurra. Si no escucharon hablar de FIDO quizá escucharon hablar de las contraseñas para la autenticación de los usuarios. Los registratarios tienen que entrar a la plataforma de EUID y pueden autenticarse ante los registradores por el nombre de dominio. Es seguro y eficiente. Siguiente.

Ya me quedo sin tiempo. Creo que tenemos una buena solución para la identificación de los contactos y ahora estamos entrando en que sea accesible, reduciendo el costo de la autenticación. Si les interesa el tema de EUID, o si no, pronto les interesará, no duden en contactarse con nosotros.

MICHAEL PALAGE: Gracias, Timo. Les aconsejo que busquen la presentación de Timo. Por un tema de tiempo le vamos a pasar la palabra a Jacques Latour. Tiene la palabra, Jacques.

JACQUES LATOUR: Estoy entre ustedes y las cervezas así que voy a hablar rápido. Vamos a hablar de la información del proceso de validación de información del

registratario en .CA. El proceso que usamos para verificar la información del registratario se basa en la verificación de presencia canadiense. Uno tiene que ser canadiense. Hoy por hoy, cuando hay un informe de uso indebido de un dominio ejecutamos esta verificación y le pedimos al registratario que nos dé una copia digital, un escaneo de pasaporte, certificado de nacimiento, licencia de conducir. Esto tiene dos problemas. No hay preservación de privacidad porque queda el pasaporte en la red. Hacemos lo mejor para verificar los datos y eliminarlos. Ese es el primer tema. No necesitamos toda esa información.

En segundo lugar, ningún humano puede detectar el fraude con todo el deep fake que existe hoy por hoy. Es difícil hacer esta parte. La idea es poder hacer esta verificación después de la firma y tener confianza. Tenemos presentación de credenciales digitales que preservan la privacidad. En el proceso solicitamos al registratario que utilice una billetera para cargar credenciales digitales existentes tales como BC en la Columbia Británica, que pueden tener la credencial de verificación emitida por el gobierno. Este documento está firmado. Podemos verificarlo directamente con la firma.

La meta consiste en solicitar al registratario que envíe una billetera. No el documento sino la afirmación de que es canadiense. Dice que es canadiense y tiene la firma de la entidad emisora. Luego tenemos la información que es la que se verifica. Las afirmaciones digitales preservan la privacidad de esta manera.

Ahora tenemos credenciales digitales, tenemos la afirmación. Sabemos que este documento está firmado por x entidad pero cómo confiamos en que el documento está firmado por una entidad de confianza. Hoy en el taller de DNSSEC tuvimos un panel que habló una hora sobre confianza digital y registros. Lo pueden buscar ahí.

Básicamente estamos tratando de elaborar una estructura de registros de confianza para poder verificar que la entidad es quien dice ser. Lo autorizamos a emitir la credencial correspondiente. Cuando tenemos la credencial firmada del gobierno de la Columbia Británica vemos que es confiable en Canadá para emitir esta credencial y por ende esa información es auténtica. Todo tiene que ser firmado, verificado y hay confianza luego en todo lo demás. Eso es todo.

MICHAEL PALAGE: Gracias. Literalmente a horario, en el final de la sesión. Quisiera pedirles a los colegas de la organización de la ICANN si podemos seguir un par de minutos para ver si hay alguna pregunta de la sala.

MICHELLE DESMYTER: Cinco minutos.

MICHAEL PALAGE: ¿Hay alguna pregunta en la sala o en línea? Por favor, hagan la pregunta. Si no hay ninguna pregunta que surja después de estas presentaciones, si surge alguna a posteriori dirijan las preguntas al

personal de At-Large, staff@atlarge.icann.org y nosotros nos vamos a hacer cargo de hablar con los panelistas correspondientes y a enviarles las respuestas.

AVRI DORIA: Quisiera hablar de la pregunta de Alan Greenberg en el pod de preguntas y respuestas. Básicamente decía cuáles son los costos asociados del VLEI. No exactamente pero en un orden de magnitud. No sé si hay alguien que pueda responder. Karla, bien. Adelante.

KARLA MCKENNA: ¿VLEI o LEI?

MICHAEL PALAGE: Quizá podría decir ambos, por favor, porque con LEI hay un costo de recuperación del mecanismo cubierto.

KARLA MCKENNA: Tenemos entre 30 y 40 emisores de LEI. Uno de los estatutos sobre el que se fundó GLEIF es que el sistema tiene que operar para la emisión y registro de LEI en un principio de recuperación de costos. Cada uno de los emisores presenta anualmente sus números de recuperación de costos y eso afecta a lo que pueden cobrar para poder hacer la validación, emitir y mantener los LEI. El rango está entre muy, muy, muy bajo para registración para algunos de los emisores en los 20.

Llega muy comúnmente a los 50 dólares. Llega a los cientos de dólares según el tipo de organización que haya que investigar. Las organizaciones como Trust Pools y distintos tipos de sociedades pueden obtener LEI. En VLEI tenemos un emisor calificado y se cobran unos 200 dólares por la emisión del VLEI.

AVRI DORIA: Muchísimas gracias por su respuesta. Si no hay ninguna otra pregunta, en un punto Hadia levantó la mano y quería estar segura de que no se vaya frustrada. Si tiene la pregunta, tiene la posibilidad de hacerla ahora, Hadia. Me imagino que no. Muy bien. Le paso la palabra a Michael.

MICHAEL PALAGE: Gracias. Jonathan.

JONATHAN ZUCK: Jonathan Zuck, presidente de ALAC. Disfruté todas estas presentaciones y tengo curiosidad de cuál es el nivel de integración de los registradores hoy porque obviamente en el espacio de gTLD son parte integral de los múltiples registradores de TLD y deberían integrar este tipo de tecnología mientras tratan de utilizar esta verificación. ¿Es una caja negra? ¿Qué tipo de interacción tienen con los registradores? No sé a quién preguntarle esto francamente pero me quedé pensando.

MICHAEL PALAGE: Jacques, Jaromir y quizá Timo.

JACQUES LATOUR: El feedback del registrador es que funcione, que sea de bajo coste y que sea estándar. Ahí lo veremos. Por eso ven registros que están trabajando en esto y haciéndolo funcionar. Hay que empezar en algún lado y después replicarlo. No hace falta hacer la ingeniería completa.

JAROMIR TALÍŘ: No hace falta hacer nada. Si les decimos que nos ocupamos, estarán felices.

TIMO VÖHMAR: Básicamente es igual para nosotros. La plataforma de EUID es muy nueva. No hemos comenzado todavía el tema con los registradores.

JONATHAN ZUCK: Es hipotético entonces en cuanto a los registradores hoy por hoy. Todavía no participan.

TIMO VÖHMAR: Venimos hablando desde hace tiempo. Saben lo que viene. Están preparados. Vamos a tratar de que sea lo más barata y sencilla posible la integración.

AVRI DORIA: Jonathan, quizá quiera ver la presentación porque varios de los ccTLD hablaron de en qué medida han incorporado este protocolo o tal arquitectura o que están trabajando en tal o cual pero pareciera que están empezando a ganar momentum. Esa es una de las cosas que yo pensaba recopilar de esta mesa. Quién está usando qué y dónde. No sé cuánta información se va a poder recopilar pero quiero entender esto.

MICHAEL PALAGE: Bruce.

BRUCE TONKIN: Un contraste de madurez. La identificación de empresas en Australia viene utilizándose desde hace 20 años. La de los registratarios es de hace dos años en Australia.

MICHAEL PALAGE: Creo que excedimos nuestro tiempo asignado extendido. Gracias a los panelistas, asistentes, la organización, por un debate muy bueno, constructivo e interesante.

AVRI DORIA: Gracias.

[FIN DE LA TRANSCRIPCIÓN]