MUESTRA[1] PRELIMINAR DEL DESARROLLO DEL PROGRAMA PRESENTADA POR EL GRUPO ASESOR PARA LA ZONA DE DOMINIOS DE ALTO NIVEL DE ALTA SEGURIDAD (HSTLD)

[1] Muestra del desarrollo tomada del espacio wiki del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) y del listado de correo electrónico, el día 17 de febrero de 2010.

ESTATUS DE ESTE DOCUMENTO

La presente es una muestra del desarrollo de actividades del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG), que ya han sido completadas o están en curso. El trabajo preliminar que se presenta en este documento refleja un esfuerzo de desarrollo continuo entorno a un programa voluntario designado para respaldar estándares de control e incentivos para incrementar la confianza en los Dominios de Alto Nivel (TLD) que elijan participar en el programa.

RESUMEN

Presentamos este informe a la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para la recepción de comentarios, como parte de la labor continua en el desarrollo de la Guía para el Solicitante para los Nuevos Dominios Genéricos de Alto Nivel (gTLDs). El trabajo reflejado en este informe se considera como “trabajo en progreso”, a medida que desarrollamos un programa voluntario de Dominios de Alto Nivel (TLD) de Alta Seguridad.

ESTÁNDARES DE DOCUMENTACIÓN

Como muestra del desarrollo, el contenido del presente documento es una combinación de breves descripciones y el estado real actual de los elementos del programa que actualmente se están desarrollando en el programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Para ayudar a hacer la distinción entre las descripciones de los elementos del programa y el contenido real del desarrollo del programa, las descripciones de los elementos del programa se encuentran en texto normal y el contenido que corresponde al desarrollo del programa se encuentra en letra cursiva.

Contenidos

1.0 RESUMEN EJECUTIVO

El trabajo inicial sobre un programa voluntario que consiste en normas/estándares de control e incentivos para incrementar la confianza en los Dominios de Alto Nivel (TLD) que decidan participar en el programa, ocurrió antes de la reunión pública internacional que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebró en Seúl. Durante el período de tiempo previo a la reunión de Seúl, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) creó un documento conceptual esbozando las ideas iniciales sobre cómo se podría lograr dicho programa voluntario. El documento conceptual fue publicado como un componente de la versión 3 del Borrador de la Guía para el Solicitante para los nuevos Dominios Genéricos de Alto Nivel (gTLD), al cual puede accede mediante el siguiente enlace:

http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf

Gran parte de la respuesta de la comunidad al documento conceptual fue positiva. Para continuar apoyando el desarrollo del concepto, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha invitado a los miembros de la comunidad a participar en un Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG). El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) está actualmente conformado por miembros del personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los miembros de la comunidad que han expresado interés en colaborar con el programa, así como por individuos que son expertos en la materia de disciplinas relacionadas con el programa (por ejemplo: seguridad, auditoría, programas de certificación). El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) se reúne regularmente para avanzar sobre los conceptos introducidos en el documento original, para redactar elementos de control y requisitos del programa y para publicar un programa de acciones concretas para consideración y revisión por parte de la comunidad. Este trabajo presenta los materiales más recientes que se encuentran bajo revisión o desarrollo por parte del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG).

El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) lleva a cabo sus actividades y el desarrollo del programa mediante un proceso abierto y transparente. Esta muestra del desarrollo es un componente de este proceso. En el siguiente enlace podrá encontrar información adicional, incluyendo los participantes del grupo y grabaciones de las reuniones semanales del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG):

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

2.0 ACTIVIDADES DE DESARROLLO

Las actividades de desarrollo más significativas que tomaron lugar a partir de la reunión pública internacional que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebró Seúl, Corea incluyen:

- Formación del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) y revisión del documento conceptual original por parte de dicho grupo;
- Documentación de los requisitos y fundamentos originales de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD);
- Trabajo adicional para mejorar el contenido del documento conceptual original, incluyendo componentes fundamentales como:
    - Declaración del Objetivo del Grupo
    - Declaración del Problema de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD)
    - Declaración de los Beneficios de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD);
- Trabajo adicional para mejorar los Principios, Temas, Objetivos y Criterios de Muestra del documento conceptual original; y
- Incorporación del concepto de “tabla de calificación”.

El resto de este documento de muestra del desarrollo explicará cada una de las actividades antes mencionadas y presentará su estado actual de desarrollo como una "foto instantánea" en el tiempo. El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) utiliza sus reuniones semanales, correo electrónico y espacio wiki del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) —así como otras herramientas de colaboración—, para desarrollar el material del programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). En última instancia, el material creado por el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) será utilizado para crear los elementos clave y las acciones concretas del programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). El Grupo Asesor (AG) publicará luego el programa, para la recepción de comentarios públicos.

2.1 Formación del HSTLD AG

Se comenzó a trabajar en el mejoramiento del concepto de programa voluntario de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD), mediante el patrocinio de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para un grupo asesor que está compuesto por personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y miembros interesados de la comunidad. El grupo se formó para continuar desarrollando el material conceptual de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) voluntaria, originalmente publicado como un componente de la reunión pública internacional que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebró en Seúl Corea. La primera reunión del Grupo Asesor para la Zona

de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) fue el 6 de enero de 2010 y el grupo continúa reuniéndose una vez por semana para trabajar en el desarrollo del concepto del programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). El estatus de los esfuerzos de desarrollo realizados por el grupo, las actualizaciones del desarrollo y, en definitiva, un nuevo documento conceptual (si el programa se considera listo) serán informados en las reuniones internacionales que célebre la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

2.2 Documentación de requisitos y fundamentos originales para HSTLD

A medida que se formaba el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG), el grupo se enumeró los requisitos y fundamentos originales para el documento conceptual de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD), para ayudar al desarrollo de material central. Este material fue recolectado y referenciado en el siguiente enlace:

http://mm.icann.org/pipermail/hstld-ag/2010-January/000094.html

2.3 Generalidades del Material en Desarrollo

Una de las primeras áreas de enfoque para el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG), fue la determinación del objetivo, problemas y beneficios de dicho Grupo. Estas áreas conforman la base de un programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) bien ejecutado, a la vez que sirven como sus lineamientos generales. Por el momento, el debate del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) ha progresado más allá de estas áreas, pero las mismas serán revisadas según sea necesario, a través del esfuerzo de desarrollo general de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD).

Durante el desarrollo de las declaraciones de objetivo, problemas y beneficios, los miembros del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) sugirieron un nuevo método de presentación de informes, para los Dominios de Alto Nivel (TLD) que estén interesados en convertirse en un Dominio de Alto Nivel de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). El nuevo método de presentación de informes está basado en un concepto de “tabla de calificación”. El mismo proporciona un método para el autocertificar el cumplimiento con el programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). El Grupo Asesor (AG) evaluará este método de presentación de informes y lo comparará con otros programas de certificación, sello de confianza y demás programas de verificación similares.

Luego de que el objetivo, problemas y beneficios de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) fueron creados y discutidos, del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) se centró en los principios, temas, objetivos y criterios de muestra. Este material es el material sobre el cual se debatió más recientemente y aún está siendo desarrollado activamente.

Cada una de estas secciones será brevemente descripta a continuación, presentando con un texto normal lo que describe al material y en letra cursiva el material preliminar de trabajo del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG).

2.4 Declaración del Objetivo del Grupo

La primera tarea de desarrollo emprendida por el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) fue la de formular una declaración del objetivo de dicho Grupo. La declaración del objetivo del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) ofrece a la comunidad un estatuto de su objetivo general. Proporciona un método para comunicar el objetivo y directrices generales a la comunidad y a los miembros del Grupo. La actual declaración de objetivo del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) establece lo siguiente:

"El objetivo del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) es reunir a representantes de la comunidad para evaluar la viabilidad de un programa voluntario, normas/estándares de control e incentivos de respaldo que pudiesen ser potencialmente adoptados para proporcionar un mayor nivel de confianza y seguridad por sobre los controles de registración-autoridad básicos."

2.5 Declaración del Problema del Grupo

A medida que el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) comenzó a elaborar una declaración de objetivo adecuada, varios miembros del Grupo Asesor (AG) plantearon la cuestión de definir los problemas por cuya solución se resolvió conformar dicho Grupo, a fin de que estos problemas fueran documentados y estuviesen disponibles para la revisión de la comunidad. Este material ayudará a mantener enfocado Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG), a medida que se diseñen controles para reducir estos problemas. La declaración del problema del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) establece lo siguiente:

"Ciertos individuos/organizaciones han buscado explotar las vulnerabilidades dentro de la tecnología del Sistema de Nombres de Dominio (DNS) y las prácticas comerciales de algunas autoridades de registración, para propósitos/fines inadecuados y/o ilícitos. La explotación de estas vulnerabilidades ha amenazado la seguridad y estabilidad de Internet y ha impactado negativamente en la confianza que los usuarios tienen cuando utilizan Internet.

Existen varias partes interesadas:

1. *Los Registrantes que desearían estar seguros de que el nombre que registran no sea secuestrado a través de ver comprometido al registrador/registro/su propia cuenta. (Incluyendo al Sistema de Nombres de Dominio —DNS—, WHOIS, etc.)*

2. *Los Registradores que desearían ser capaces de otorgar garantías razonables a los Registrantes de que los perjuicios mencionados en el ítem Nro. 1 no ocurrirán porque ellos tienen controles. Para que ello suceda, necesitan la cooperación tanto del Registrante como del Registro.*

3. *Los Registros también quisieran como contar con la seguridad mencionada en el ítem Nro. 1 y esto requiere de la cooperación tanto del Registrante como del Registrador.*

4. *Los usuarios finales desearían saber que cuando escriben un determinado nombre de dominio o navegan a partir de páginas marcadas como favoritas, etc. en realidad acceden al dominio correcto y que el Sistema de Nombres de Dominio (DNS), etc. no han sido secuestrados.*

5. *Los usuarios finales desearían entender que un nombre de dominio registrado dentro de un Dominio Genérico de Alto Nivel (gTLD) particular, está sujeto a normas/estándares de registración, políticas y procedimientos que tengan por objeto reducir la conducta maliciosa por tales registrantes."*

2.6 Declaración de los Beneficios del Grupo

La última área para conformar los cimientos del desarrollo del programa hasta la fecha es el desarrollo de una declaración de beneficios del Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG). La finalidad última del material de beneficio es ayudar a la comunidad a entender cuáles son los beneficios que se podrían lograr mediante la adhesión a un programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Este material no pretende ser un análisis integral de los beneficios empresariales/comerciales. En lugar de ello, tiene por objeto ofrecer los beneficios generales de la comunidad, desglosados por los grupos que más se verían impactados por el programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Este material de beneficio de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) es actualmente el siguiente:

"Beneficio para los Registros:

Ry1. *demostrar que tienen un alto nivel de continuidad, seguridad e integridad operacional mediante un proceso de auditoría.*

Ry2. *demostrar que realizan operaciones comerciales que han sido revisadas y han cumplido con las normas/estándares de integridad organizacional, operacional y financiera.*

Ry3. *demostrar que tienen el procesamiento de datos, almacenamiento y métodos que cumplen altos estándares para la confidencialidad de los datos, precisión, integridad, recuperación, etc.*

Ry4. *demostrar que han implementado prácticas y medidas para mitigar los abusos del servicio de nombres de dominio y de los servicios de registración de dominios.*

Ry5. *satisfacer (Ry1) a (Ry4), que infunden confianza en los usuarios finales y registrantes respecto a que sus empresas son financieramente solventes y dignas de confianza, y garantizar que sus medidas para reducir la incidencia de dominios maliciosos registrados son aplicadas por los registradores que tramitan las registraciones para el Registro.*

Beneficios para los Registradores:

Rr1. *demostrar que han cumplido con todas las normas/estándares estándares para la continuidad, seguridad e integridad operacional que "se filtra" a partir de un registro de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) a través de un proceso de auditoría. (el "filtrado" significa que el registrador hace cumplir cualquier condición que sea impuesta al registro y que no se*

pueda cumplir sin la asistencia del registrador, por ejemplo: una condición que afecte a la interfaz registro-registrador).

Rr2. demostrar que sus operaciones comerciales han sido revisadas y cumplen con las normas/estándares de integridad organizacional, operacional y financiera que "se filtra" de un registro de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD).

Rr3. beneficiarse mediante el "filtrado" de Ry3.

Rr4. beneficiarse mediante el "filtrado" de Ry4.

Rr5. satisfacer (Rr1) a (Rr4), lo cual infunde confianza en los usuarios y registrantes respecto a que el Dominio de Alto Nivel de Alta Seguridad (HSTLD) confía en que el registrador tramite las registraciones en nombre del registro. Las normas/estándares más estrictos para el procesamiento de las registraciones también garantizan a los usuarios y registrantes que los datos de registración son precisos y que los reclamos/denuncias de abuso se procesan conforme a las prácticas estándar, etc.

Beneficio para los Registrantes:

Re1. demostrar que están dispuestos a someterse a medidas de verificación estrictas asociadas con un registro de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD).

Re2. demostrar que están dispuestos a mantener datos de registración que sean precisos/exactos (y cumplir con las medidas de control implementadas para garantizar que así sea).

Re3. demostrar que están dispuestos a aceptar los términos de servicio (TOS) y Políticas de Uso Aceptable (AUP) que enumeran los usos prohibidos, los abusos y brindan facultades al registro/registrador para suspender u adoptar otras respuestas, cuando exista un incumplimiento en dichos términos de servicio y políticas de uso aceptable.

Re4. beneficio a partir de las medidas implementadas para mitigar las registraciones de dominio maliciosos: muchas de dichas medidas hacen que sea más difícil para los atacantes el comprometer la cuenta de un registrador legítimo.

Re5. beneficio a partir de las medidas implementadas para mitigar el abuso del Sistema de Nombres de Dominio (DNS): muchas de las mismas medidas hacen que sea más difícil para los atacantes comprometer las cuentas de un registrante legítimo y luego alterar la información de configuración del Sistema de Nombres de Dominio (DNS).

Beneficio para los Usuarios:

U1. beneficio a partir de datos de registración más precisos/exactos.

U2. beneficio a partir de menos cantidad de incidentes de registraciones maliciosas y abuso del Sistema de Nombres de Dominio (DNS) entre los nombres de dominio registrados en la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD).

U3. beneficio a partir de los procesos claramente definidos para la gestión de abusos"

2.7 Concepto de "Tabla de Calificaciones"

A medida que el Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) desarrollaba el material de base anteriormente presentado, se plantearon preguntas respecto a la verificación original del proceso de certificación del documento conceptual. El documento conceptual original utilizaba un método de certificación realizado por una tercera parte, como un mecanismo para informar a la comunidad la adhesión de un Dominio de Alto Nivel (TLD) a los controles establecidos por

el programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Mediante el proceso de discusión del grupo, se introdujo un método alternativo (aunque no excluyentes entre sí) para la adopción de los controles establecidos por el programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD) por parte de un Dominio de Alto Nivel (TLD). El método alternativo está basado en el concepto de una tabla de calificación que un Dominio de Alto Nivel (TLD) puede completar para informar a la comunidad acerca de su nivel de cumplimiento de los controles correspondientes a la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). A continuación se presenta una visión muy general del concepto:

"Tabla de Calificación de Seguridad del Dominio de Alto Nivel (TLD)

Actualmente la Corporación para la Asignación de Números y Nombres en Internet (ICANN) no proporciona métricas para facultar a los registrantes para tomar una decisión informada acerca de sus opciones de registración de nombres de dominio. La Tabla de Calificación de Seguridad sería un concepto que podría integrarse a las características actuales del panel de control de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

Esta tabla de calificación estaría compuesta por una matriz de criterios de control de seguridad acordados en el eje Y, y por "todos" los operadores de registro de Dominio de Alto Nivel (TLD) en el eje X. Cada casilla de la matriz cumpliría con el siguiente esquema de colores:

- *Casilla Blanca/Vacía: El operador de registro no ha brindado datos en conexión con ese elemento de control.*
- *Casilla sombreada de Amarillo: El operador de registro ha "autocertificado" su cumplimiento en relación a ese elemento de control.*
- *Casilla sombreada al 50% de Verde: Una tercera parte ha verificado el cumplimiento del registro con ese elemento de control en un momento específico, pero no ha sido capaz de establecer un cumplimiento a largo plazo.*
- *Casilla sombreada al 100% de Verde: Una tercera parte ha verificado el cumplimiento del registro con ese elemento de control durante un período de cumplimiento prolongado.*
- *Casilla sombreada de Rojo: En una circunstancia en la cual un registro haya "autocertificado" un criterio de control específico pero se hubiese encontrado en falta/incumplimiento. Se prevé que toda declaración falsa respecto a la autocertificación sería una infracción al acuerdo de registro, el cual será investigado por el personal de cumplimiento de la Corporación para la Asignación de Números y Nombres en Internet (ICANN)".*

2.8 Principios, Temas, Objetivos y Criterios de Muestra

La Sección 3.2.1 del documento conceptual original contenía detalles sobre los requisitos centrales del programa de Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Esta sección representa una recopilación de principios, objetivos y criterios que constituyen la base de los controles reales que están diseñados para mejorar la seguridad y la confianza de los Dominios de Alto Nivel (TLD). El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) ha estado trabajando para mejorar esta sección. Más recientemente, los principios originales han sido revisados y se redactó un principio adicional (que actualmente se lista como "Principio 4"), el cual está siendo debatido para el eventual agregado a los principios. El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad

(HSTLD AG) también está evaluando la "temas posibles de criterios", en un esfuerzo por llegar a un acuerdo sobre los criterios reales y los ejemplos de control de respaldo ilustrativo. Cuando esté completamente terminado, cada tema de los criterios contará con uno o más ejemplos ilustrativos de control que ofrecerán directrices/lineamientos para un adecuado control, necesario para cumplir con los requisitos de los criterios. A continuación se presenta el estado actual del desarrollo de esta sección:

"PRINCIPIO 1: el Registro mantiene controles efectivos para proporcionar garantías razonables de que la seguridad, disponibilidad y confidencialidad de los sistemas y activos de información que respaldan la Tecnología de Información (IT) crítica del registro (es decir: los servicios de registración, bases de datos del registro, administración de la zona y prestación de servicios de resolución de nombres de dominio) y las operaciones comerciales se mantienen mediante la realización de lo siguiente:

• definición y comunicación de los objetivos de desempeño/rendimiento, políticas y normas/estándares para el sistema, así como la seguridad, disponibilidad, confidencialidad y privacidad de los activos de información;
• utilización de los procedimientos, personas, software, datos e infraestructura para alcanzar los objetivos definidos conforme a las políticas y normas/estándares establecidos; y
• monitoreo/control del sistema y activos de información y adopción de medidas para lograr el cumplimiento de los objetivos, políticas y normas/estándares establecidos.

No.	*Tema*	*Objetivo*	*Posibles Temas de Criterios*	*Criterios*	*Controles Ilustrativos*
1.1	*Infraestructura de Seguridad de la Tecnología de Información (IT) del Registro*	*Elementos clave de los componentes de la Tecnología de la información (IT) que respalden la infraestructura del Dominio de Alto Nivel (TLD) que estén asegurados y apropiadamente protegidos de acceso físico o virtual no autorizado.*	· *Gestión de seguridad* · *Personal de seguridad* · *Control de acceso físico* · *Medios de almacenamiento y eliminación* · *Sistema de adquisición y controles de desarrollo* · *Controles de seguridad para la gestión de incidentes* · *Respuesta a incidentes de seguridad y presentación de informes* · *Controles de interfaz* · *Gestión de acceso al sistema Seguridad de la red* · *Seguridad de aplicación Requisitos de cifrado* · *Pruebas periódicas de vulnerabilidad y ejercicios de respuesta* · *Proceso de liberación del*		

			software del sistema · *Controles de gestión del servicio de resolución de nombres (por ejemplo: integridad de la zona del Sistema de Nombres de Dominio —DNS— y monitoreo/vigilancia disponible para el servidor de nombres, ...)* · *Plan de despliegue de Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC)* · *Canales de comunicaciones seguros (conexiones autenticadas y encriptadas con los registradores)* · *Gestión de activos de información (precisión /integridad/disponibilidad de la base de datos, servicios de zona, datos de registración y otros datos del cliente)*		
1.2	*Disponibilidad de la Infraestructura de Tecnología de Información (IT) del Registro*	*Los servicios del Dominio de Alto Nivel (TLD) están disponibles para el uso por contrato o compromiso.*	· *Acuerdos de nivel de servicio* · *Disponibilidad del servicio Whois* · *Nivel de desempeño/rendimiento del servicio Whois* · *Tiempos de respuesta del servicio Whois* · *Exactitud e integridad de Whois Monitoreo/vigilancia de disponibilidad* · *Custodia de datos de registración y transacción, incluyendo cronograma, especificaciones, transferencia y Verificación de Seguridad de la custodia* · *Recuperación de desastres y*		

			plan de continuidad de negocios (prácticas ante fallas, incluyendo planes para mantener el servicio de resolución de nombres ante el evento de una falla empresarial) y ejercicios · *Controles ambientales (energía y aire acondicionado, protección contra incendios)* · *Controles de seguridad del cableado*		
1.3	*Confidencialidad y Privacidad de los Datos Sensibles*	*La información de propiedad, gestionada o transferida a través del Dominio de Alto Nivel (TLD) ha sido designada como confidencial y está protegida conforme al compromiso asumido o según lo acordado. La información personal recopilada por el operador del Dominio de Alto Nivel (TLD) es recopilada, utilizada, conservada, divulgada y destruida apropiadamente, de acuerdo con las leyes de protección de datos relevantes de la jurisdicción del operador de registro.*	· *Clasificación adecuada de la información confidencial y de identificación personal* · *Políticas para la recopilación, utilización, retención, acceso y divulgación de datos* · *Datos en reposo y en tránsito* · *Acceso a la información por parte de terceros* · *Requisitos de cifrado* · *Controles de gestión para las llaves de firma* · *Controles de acceso físico y virtual* · *Separación de las obligaciones* · *Monitoreo/vigilancia del sistema* · *Controles de seguridad personal*		

PRINCIPIO 2: El Registro mantiene controles efectivos para ofrecer una garantía razonable de que el procesamiento de las funciones centrales del Registro están autorizadas, sean precisas, completas y realizada de una manera oportuna, conforme a las políticas y normas/estándares establecidos. La identidad de las entidades participantes es establecida y autenticada.

No.	*Tema*	*Objetivo*	*Posibles Temas de Criterios*	*Criterios*	*Controles Ilustrativos*
2.1	*Verificación de Seguridad del*	*Las credenciales del operador de registro se*	*· Indagación de la organización del*		

	Registro	*ponen a disposición para demostrar la identidad de la persona jurídica que opera el Dominio de Alto Nivel (TLD).*	*REGISTRO, incluyendo:* *- Antecedentes de los funcionarios* *- Dirección verificable* *- Dirección de correo electrónico verificable* *- Números de teléfono verificables* *- Acta constitutiva* *- Certificado de formación* *- Documentos estatutarios* *- Nombre Comercial (es decir, nombre asumido)* *- Registración de nombre comercial* *- Documentos societarios* *- Licencia comercial* *· Cobertura del seguro* *· Capacidad financiera* *· Requisitos de revalidación* *· Procesos de indagación para empleados*		
2.2	*Verificación de Seguridad del Registrador*	*La identidad del Registrador es designada y establecida antes del inicio de las operaciones*	*· Indagación de la organización del REGISTRADOR sobre los temas señalados en 2.1* *· Estatus de acreditación del Registrador* *· Requisitos de revalidación*		
2.3	*Integridad de los Procesos del Registro*	*Los datos del Dominio de Alto Nivel (TLD) son coherentes y correctos a nivel del Registro del Dominio de Alto Nivel (TLD)*	*· Registración y mantenimiento de nombres de dominio* *· Mantenimiento, precisión, carácter completo e integridad de los datos públicos de Whois* *· Indagación de los nuevos registradores* *· Procesos de monitoreo/vigilancia continuos* *· Revisión de control de calidad de los datos del Registrador (y resultados de auditoría de custodia de datos)* *Proceso de resolución de disputas*		
2.4	*Política y Cumplimiento Antiabuso*	*Establecer controles efectivos para reducir la conducta maliciosa por medio de Registradores y Registrantes*	*· Controles Anti-phishing y anti-spoofing para los nuevos Dominios de Alto Nivel (TLD)* *· Puntaje por parte de una tercera*		

			parte independiente a partir de analistas y laboratorios anti-phishing y anti-malware · *Acuerdo del Nivel de Servicio (SLA) en base al porcentaje de dominios maliciosos por "medida unitaria" de registraciones (por ejemplo: 1000, 5000, 10.000 dominios)* *Política de servidores de nombre huérfanos (declaración de acciones que se tomarán para identificar y corregir servidores de nombres huérfanos)* · *Puntos de contacto de abuso con un proceso de respuesta documentado que sea oportuno y auditable* · *Definición de uso malicioso (conducta), prohibición explícita de la conducta maliciosa en el acuerdo de los términos de servicio del registrante* · *Proceso de Suspensión Rápida de Dominios* · *Amplio proceso y respaldo de Whois* · *Plan de despliegue de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y de IPv6* · *Monitoreo de zona en tiempo real (por ejemplo, para detectar actividades sospechosas, o fast flux)* · *Informes mensuales de actividad maliciosa informada al registro (como suplantación de identidad y redes de robots) y compromiso para hacerles frente si los resultados son altos (en relación con otros registradores que hacen negocios con este registro)*		

PRINCIPIO 3: El Registro deberá mantener controles efectivos para ofrecer una garantía razonable de que el procesamiento de las funciones centrales de los Registradores están autorizadas, sean precisas, completas y realizada de una manera oportuna, conforme a las políticas y normas/estándares establecidos. La identidad de las entidades participantes es establecida y autenticada

No.	*Tema*	*Objetivo*	*Posibles Temas de Criterios*	*Criterios*	*Controles Ilustrativos*
3.1	*Verificación de Seguridad del Registrante*	*La identidad del Registrante es verificada y establecida antes de que el Registrador otorgue el nombre de dominio.*	· *Indagación de temas de organización señalados en 2.1* · *Autoridad del Registrante para registrarse en el Dominio de Alto Nivel (TLD)* · *Usuarios comerciales exentos de registraciones Proxies/Anónimas (el solicitante deberá probar que es una persona física, la organización debe mostrar causa o justificación para el anonimato)*		
3.2	*Integridad de los Procesos del Registrador*	*Los datos son coherentes y correctos a nivel del Registrador*	· *Registrador que autentique a nuevos registrantes a través de los procesos acordados* · *Confirmación del registrador de que los datos de registración son precisos/exactos y están completes* · *Vigilancia del Registrar sobre los datos de registración por exactitud y carácter completo* · *Autenticación del registrador de los datos de registración para cada transacción* · *Confirmación del registrador de cambios en los datos de registración* · *Rechazo/suspensión con causa de los datos de registración (incompletos, falsos o inexactos)* · *Whois Amplio* · *Eliminación de los datos de registración por parte del registrador* · *Registrar la eliminación de los datos de registro* · *Procesos continuos de monitoreo/vigilancia* · *Revisión periódica de control de calidad de los datos del registrante* · *Procesos de baja y objetivos de*		

			tiempos apropiados (por ejemplo, media del tiempo de recuperación —MTTR—)		

PRINCIPIO 4: Se espera que los Registrantes en una Zona de Alta Seguridad, la información actualizada y precisa y se comprometan a abstenerse de las actividades diseñadas para confundir o engañar al público que utiliza la Internet.

No.	*Tema*	*Objetivo*	*Posibles Temas de Criterios*	*Criterios*	*Controles Ilustrativos*
4.1	*Precisión de los Datos del Registrante*	*Los Registrantes brindan información de identidad y localización actualizada y precisa/exacta.*	· *La información de localización del Registrante de los datos de WHOIS es brindada al registro* · *La información de contacto es suministrada al registro* · *Ausencia de proxies (representaciones)*		
4.2	*Conducta del Registrante*	*Los Registrantes se comprometerán de forma explícita a acatar las políticas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), así como cualquier obligación adicional creada a través de la implementación de las normas/estándares de la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD)*	*Código de Conducta*		

3.0 PRÓXIMOS PASOS

El Grupo Asesor para la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD AG) continuará desarrollando material en un esfuerzo por mejorar el documento conceptual original sobre la Zona de Dominios de Alto Nivel de Alta Seguridad (HSTLD). Los próximos pasos inmediatos incluyen —pero no se limitan a—, la continuación de las reuniones semanales del grupo, la reunión en Nairobi y el desarrollo continuo del material clave del programa, incluyendo:

- Material de base (fundamentos);
- El concepto de "tabla de calificación" *versus* otras opciones alternativas;
- Principios, objetivos, criterios y ejemplos ilustrativos; y
- Gobernanza y actores del programa en general.

Tal como se mencionara anteriormente, durante las reuniones internacionales de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se publicarán muestras del desarrollo y actualizaciones del documento conceptual original.