Article #: 030030	Date: 15 de Noviembre 2011
Article Name: Pregunta de evaluación #30: Política de Seguridad	AGB Reference: none
Version #: v01	Category: Knowledge Article – Evaluation Questions

Notas Complementarias

Mejores Prácticas Sugeridas

Texto de la Pregunta

1. NOTAS COMPLEMENTARIAS

15 de noviembre de 2011

1.1 For Question 30(a):

- Los niveles de seguridad son definidos por el solicitante. Es necesario que el solicitante enumere los compromisos que asumirá para con sus registrantes, basándose en los niveles de seguridad definidos. Asimismo, debe suministrarse una breve descripción de cada uno de los compromisos enumerados.
- El informe de evaluación independiente debe demostrar controles de seguridad efectivos sobre la estructura de IT que se utilizará para la ejecución de las operaciones del registro. La respuesta del solicitante debe abordar todas las áreas resaltadas que requieran mediación según el informe de evaluación independiente. Tenga en cuenta que la ICANN se abstendrá de publicar el informe de evaluación independiente.

1.2 Para la Pregunta 30 (b), deben presentarse políticas y procedimientos de seguridad que se focalicen exclusivamente en las operaciones de registro del solicitante. Debido a que esta información es delicada, la ICANN se abstendrá de publicar la política de seguridad del solicitante.

2. MEJORES PRÁCTICAS SUGERIDAS:

15 de noviembre de 2011

2.1 Los solicitantes deben leer cada pregunta de la evaluación por completo, incluyendo notas, criterios y pautas de calificación. La respuesta debe abordar los criterios especificados, e incluir fundamentos detallados que demuestren un exhaustivo entendimiento de los criterios (es decir, que demuestren su trabajo).

2.2 En caso de utilizar acrónimos, los solicitantes deben desglosarlos la primera vez que se utilicen, aun cuando dichos acrónimos se refieran a un término, producto o servicio común.

2.3 Los solicitantes que propongan la tercerización de función(es) de sus operaciones de registro, deben abordar todos los criterios especificados en cada pregunta pertinente, como así también incluir fundamentos detallados que demuestren un exhaustivo entendimiento de los criterios (es decir, que demuestren su trabajo).

2.4 La mera presentación de un Currículum Vitae (CV/Hoja de Vida) no se tendrá por demostración fehaciente de las capacidades técnicas/operativas, como tampoco será "prueba" fehaciente de que se cuenta con los recursos necesarios. El solicitante debe suministrar una explicación detallada del plan de recursos, e incluir áreas tales como recursos requeridos para administrar/ejecutar una función, habilidades requeridas, cronograma de contrataciones, etc. Los CV podrán ser utilizados como información complementaria al plan de recursos propuesto.

2.5 En el caso de hacer referencia a políticas o procedimientos en una respuesta, los solicitantes deben suministrar un resumen de las políticas o los procedimientos mencionados. Los solicitantes no deben adjuntar copias de las políticas o los procedimientos mencionados, salvo cuando se las solicite específicamente.

2.6 Si el solicitante propone el uso de un software diseñado específicamente para las necesidades de su cliente, deberá aclarar el alcance y la extensión de dicha adaptación, incluyendo el proceso de desarrollo del software. El propósito de la aclaración es ayudar a los paneles evaluadores a comprender la integridad del software customizado/adaptado a las necesidades del cliente.

3. TEXTO DE LA PREGUNTA:

(a) Suministrar un resumen de la política de seguridad y procedimientos para el registro propuesto, incluyendo pero no limitándose a:

- Indicación de cualquier informe de evaluación independiente que demuestre las capacidades de seguridad y disposiciones para llevar a cabo informes periódicos de evaluación independiente que comprueben las capacidades de seguridad;
- Descripción de cualquier nivel de seguridad aumentada o capacidades acordes con la naturaleza de la cadena de caracteres de dominio genérico de alto nivel (gTLD) solicitado, incluyendo la identificación de cualquier norma vigente de seguridad internacional o relevantes a la industria que el solicitante se comprometa a seguir (se debe suministrar referencia al sitio).
- Lista de los compromisos contraídos con los registrantes relativos a los niveles de seguridad.

Para ser elegible para una puntuación de 2, las respuestas también deben incluir:

- Evidencia de un informe de evaluación independiente que demuestre controles de seguridad eficaces (por ejemplo, ISO 27001).

Un resumen de lo anterior no debe exceder las 20 páginas. Tenga en cuenta que es requisito presentar la política de seguridad completa del registro de conformidad con 30(b).

(b) Proporcionar la política de seguridad completa y procedimientos para el registro propuesto, incluyendo pero no limitándose a:

- Sistema (datos, servidores, aplicaciones o servicios) y el control de acceso a la red, garantizando que los sistemas sean mantenidos de manera segura, incluyendo detalles de cómo se supervisan, conectan y copian para seguridad;
- Recursos para garantizar la integridad de las actualizaciones entre los sistemas de registro y los servidores de nombres, y entre los servidores de nombres, si los hubiere;
- Informes de evaluación independientes que demuestren las capacidades de seguridad (presentados como adjuntos), si los hubiere;
- Aprovisionamiento y otras medidas que atenúen los riesgos que presentan los ataques de denegación de servicio;
- Políticas, planes y procesos de respuesta a los incidentes informáticos y de red;
- Planes para minimizar el riesgo de acceso no autorizado a sus sistemas, o de alteraciones fraudulentas de datos de registro;
- Mecanismos de detección de intrusos, un análisis de amenazas para el registro propuesto, las defensas que se implementarán contra esas amenazas y la previsión de actualizaciones periódicas del análisis de amenazas;
- Detalles de capacidades de auditoría en todos los puntos de acceso a la red;
- Enfoque de seguridad física;
- Identificación del departamento o grupo responsable por la organización de la seguridad del registro;
- Averiguación de antecedentes de todo el personal de seguridad;
- Descripción de las principales amenazas de seguridad que han sido identificadas para la operación del registro; y
- Planes de implementación de recursos para la implementación inicial de, y el mantenimiento continuo para, este aspecto de los criterios (cantidad de personal y descripción de las funciones del personal asignado a esta área).