ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-014 **FECHA DE EFECTIVIDAD:** 7 de noviembre de 2016

TEMA: Manejo de *Firewalls*

DESCRIPCIÓN DE LA POLÍTICA

El propósito de esta política es establecer que toda agencia debe tener, al menos, un dispositivo o conjunto de dispositivos conocido como *firewall* que controle el acceso al internet y personal capacitado para el manejo del mismo.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.,* Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos. Asimismo, aplica a cualquier otro organismo gubernamental que esté conectado a la Red Interagencial.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable por la actualización de esta política.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico deberá seguir las políticas aquí dispuestas sobre manejo de *firewall*. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos internos para cumplir la política aquí delineada.

A. Protección Mínima

1. Toda agencia debe tener un *firewall* protegiendo, como mínimo, su conexión a internet.
2. Si el *firewall* requiere algún licenciamiento, el mismo debe estar vigente.
3. Se deben hacer resguardos periódicos de la configuración del *firewall* en un sistema de almacenamiento alterno (no en el mismo dispositivo). El acceso a este resguardo debe estar restringido sólo al personal responsable de administrar el equipo.

B. Personal

1. Toda agencia debe tener personal capacitado y adiestrado en seguridad y en el manejo de *firewalls*. En caso de delegarse a un tercero, éste debe estar capacitado y certificado en seguridad y manejo de *firewalls*.
2. Típicamente el personal de sistemas de información está demasiado ocupado trabajando con asuntos de mantenimiento y soporte de los sistemas informáticos y la seguridad es un tema sumamente complejo y sensitivo que, en muchas ocasiones, requiere personal especializado. Así las cosas, en agencias donde la complejidad de la seguridad lo requiera por necesidad de cumplimiento de regulaciones federales, tales como HIPAA, SOX, FISMA y otras leyes análogas, es recomendable que exista un Oficial de Seguridad Informática, Gerente de Seguridad Informática, Especialista en Seguridad Informática o sus equivalentes, debido a los retos técnicos que, regularmente, supone la implementación de políticas y controles para tal cumplimiento.
3. Un candidato para las posiciones antes mencionadas debe tener una combinación entre educación, experiencia y adiestramiento para ser cualificado como experto en seguridad.[1]
    a. Oficial/Especialista en Seguridad Informática
        i. El candidato debe poseer al menos un bachillerato en ingeniería (computadoras, telecomunicaciones o campos relacionados), ciencias de computadoras o sistemas de información de una universidad acreditada.
        ii. Es altamente deseable que el candidato posea alguna de las siguientes certificaciones: CEH[2], OSCP[3], CHFI[4]o su equivalente.
        iii. El candidato debe tener cinco (5) o más años de experiencia en tareas relacionadas a la seguridad y al cumplimiento de regulaciones federales.
    b. Gerente de Seguridad Informática
        i. El candidato debe poseer al menos un bachillerato en ingeniería (computadoras, telecomunicaciones o campos relacionados), ciencias de computadoras o sistemas de información de una universidad acreditada.
        ii. Es altamente deseable que el candidato posea alguna de las siguientes certificaciones: CISSP[5] o su equivalente; GIAC[6]o su equivalente; CISM[7] o su equivalente.
        iii. Diez (10) años o más de experiencia en el campo de las tecnologías de información con historial sólido en seguridad de la información y en el área de cumplimiento de regulaciones federales y, al menos, cinco (5) años en experiencia gerencial.

C. Adiestramientos

1. La agencia es responsable de proveer notificaciones a toda la gerencia y los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes. A tales fines, deberán celebrar charlas periódicas, para orientar al personal de las políticas y controles de seguridad establecidos.
2. El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
4. La agencia es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

D. Reglas Mínimas

1. *Firewalls* Perimetrales
    a. Denegar todo tráfico que no esté explícitamente permitido en ambas direcciones (*inbound* and *outbound*)
    b. Permitir de salida (*outbound*) sólo los puertos que se utilizan
        i. Ejemplo
            1. Acceso a Internet
                a. DNS (UDP y TCP 53) a DNS de la red interagencial (típicamente sólo el DNS interno de la agencia es el que debe tener acceso a DNS)
                b. HTTP (80)
                c. HTTPS(443)
2. Filtros de Contenido de Internet
    a. Deben poseer, al menos, una política base que bloquee pornografía y que aplique a TODO el personal.

E. Leyes y Reglamentos

1. Las políticas y procedimientos de seguridad deberán estar de acuerdo con la legislación y reglamentación vigentes.

EXENCIONES

Ninguna

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Firewall – un dispositivo o combinación de dispositivos configurados para permitir, denegar y/o cifrar entre los diferentes segmentos de seguridad, basado en una serie de reglas u otros criterios.

FISMA – Federal Information Security Management Act, 44 USC § 3541 *et seq*. Es una legislación federal que define una plataforma comprensiva para proteger información, operaciones y activos del gobierno en contra de amenazas naturales o realizadas por el hombre. FISMA fueintegrada al "Electronic Government Act of 2002", 44 USC § 101 *et seq*.[8]

HIPAA – Health Insurance Portability and Accountability Act, Pub.L. No. 104-101, 110 Stat. 1936 (1996). La Oficina de Derechos Civiles tiene la responsabilidad de hacer cumplir la Regla de Privacidad de la Ley HIPAA, la cual protege la información de salud individualmente identificable; la Regla de Seguridad HIPAA, la cual establece los estándares nacionales para la seguridad electrónica de la información de salud protegida; la Regla de Notificación de Violación de Seguridad, la cual requiere que las entidades y los asociados de negocio cubiertos a proveer una notificación luego de una violación de seguridad de la información de salud protegida; y las disposiciones sobre confidencialidad de la Regla de Seguridad del Paciente, la cual protege la información de identidad utilizada para analizar los eventos de seguridad del paciente y mejorar la seguridad del paciente.[9]

SOX – The Sarbanes-Oxley Act, Pub. L. No. 107-204,116 Stat. 745(2002), también conocida como Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. Se puso en efecto en julio de 2002 e introdujo grandes cambios a la regulación de la gobernanza corporativa y la práctica financiera.

ANEJOS

Ninguno

REFERENCIAS

POLITICA NÚM. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Corporate Firewall Policy [Pdf Format].(2008). In www.shortinfosec.net.Retrieved from http://www.shortinfosec.net/2008/01/downloads.html
Ley Sarbanes-Oxley.(Jan 12, 2015).In http://www.sec.gov. Retrieved fromhttp://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

---

[1]Sample-Job-Descriptions-Complete. In https://msisac.cisecurity.org
[2]EC-Council Certified Ethical Hacker http://www.eccouncil.org/
[3]Offensive Security Certified Professional https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
[4] EC-Council Computer Hacking Forensic Investigator http://www.eccouncil.org/certification/computer-hacking-forensics-investigator
[5]Certified Information System Security Professional https://www.isc2.org/cissp/default.aspx
[6] Global Information Assurance Certification http://www.giac.org/
[7]Certified Security Information Manager http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
[8] http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
[9]http://health.state.tn.us/hipaa/