



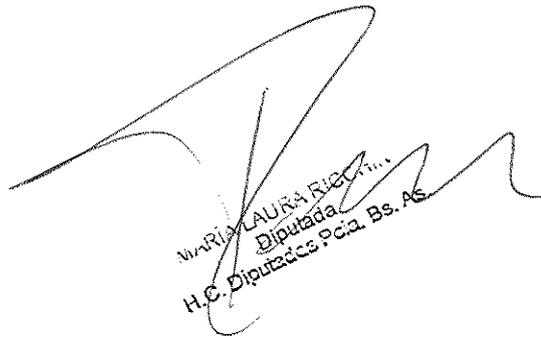
*Honorable Cámara de Diputados
de la Provincia de Buenos Aires*

PROYECTO DE RESOLUCION

**LA HONORABLE CAMARA DE DIPUTADOS
DE LA PROVINCIA DE BUENOS AIRES**

RESUELVE

Adherir y declarar de **Interés Legislativo** los actos, actividades y jornadas de concientización que se desarrollen con motivo de la conmemoración del **Día Mundial de la Seguridad de la Información**, instaurado el 30 de noviembre.


MARIA LAURA RICCIO
Diputada
H.C. Diputado, Pcia. Bs. As.



*Honorable Cámara de Diputados
de la Provincia de Buenos Aires*

FUNDAMENTOS

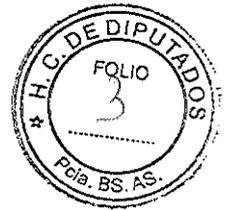
El presente proyecto pretende que el Poder Ejecutivo declare de **Interés Provincial** los actos, actividades y jornadas de concientización que se desarrollen con motivo de la conmemoración del **Día Mundial de la Seguridad de la Información**, instaurado el 30 de noviembre.

Bajo el nombre de Computer Security Day, como iniciativa de la Association for Computing Machinery (ACM), con el objeto de concientizar sobre la importancia de la seguridad de la información y de los sistemas y entornos que operan en ella.

La utilización de las Tecnologías de la Información y de la Comunicación (TIC) como medio para almacenar, transferir y procesar información se ha visto incrementada exponencialmente en los últimos años, llegando a convertirla en un elemento indispensable para el funcionamiento de la sociedad actual. A raíz de esto, la información se ha transformado en un activo de gran valor, que debe protegerse garantizando su integridad, confidencialidad y disponibilidad.

En el marco de esta celebración, el Departamento de Seguridad Informática de la Universidad Nacional de Luján le acerca una serie de buenas prácticas que puede aplicar para resguardar la información que utiliza en su actividad diaria.

Debido a que en la actualidad los ciberdelincuentes no escatiman esfuerzos a la hora de cometer sus delitos, y afectan todo tipo de empresas - incluso medianas y pequeñas- por representar una fuente de lucro económico bastante atractiva, Microsoft hace siete recomendaciones para contribuir a la protección de la información en las organizaciones:



*Honorable Cámara de Diputados
de la Provincia de Buenos Aires*

Infraestructura robusta: Para tener una buena seguridad hay que contar con una plataforma fuerte, lo cual implica varios aspectos: arquitectura, diseño de un esquema de protección, operaciones y prácticas humanas seguras, además de una administración de riesgos.

Arquitectura: Resulta relevante tener clara la finalidad de la arquitectura tecnológica de la plataforma. Es como cuando se habla del diseño de una cárcel o una base militar. Siempre debe estar considerada la finalidad del 'edificio', para lo cual resulta útil hacerse preguntas como ¿son criminales de alta peligrosidad? o ¿qué información y objetos estarán dentro de un campo militar?.

Diseño: El sistema debe estar diseñado como un todo, es decir, como un conjunto de componentes asegurados de manera separada. Una infraestructura segura debe considerar un diseño general de la solución, con énfasis o especial atención en la protección de los datos que alberga cada uno de los componentes del sistema por separado: servidores, computadores, la red, dispositivos de comunicación, entre otros.

Operaciones seguras: Configurar un nuevo servicio en línea o dar de alta a un usuario implica la interacción con un nuevo sistema, y esto se debe hacer de una forma segura.

Mejores prácticas: Se debe tener una visión clara de las acciones que han tenido buenos resultados anteriormente para definir la mejor manera de operar. Tener claridad sobre estos procesos como referentes de mejora puede ser muy beneficioso. Si no se traza un objetivo, no hay oportunidad de mejorar. Lo mismo sucede en la seguridad.

Administración de riesgos: Todas las empresas son diferentes. Las industrias, el alcance de las amenazas, así como las exposiciones al riesgo son



*Honorable Cámara de Diputados
de la Provincia de Buenos Aires*

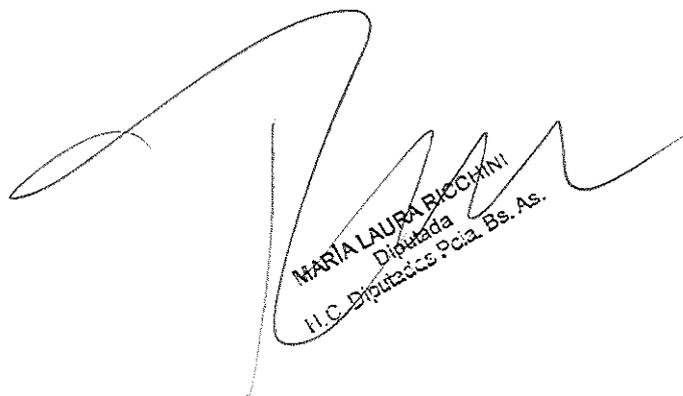
diferentes, por ende es importante tener un referente. ¿Cuál sería la mejor recomendación para una pyme? Depende de la naturaleza de su negocio y del nivel de confidencialidad de la información que maneja. Trazar un horizonte de riesgos le da claridad a las empresas para evaluar hasta dónde quieren optimizar su sistema y a qué le dan prioridad.

Cómputo en la nube: La nube está diseñada para garantizar la seguridad de los procesos. Aunque las operaciones y configuraciones las realiza el proveedor, la arquitectura de la nube ya viene armada, lo cual disminuye la exposición al riesgo.

Algunas de las iniciativas de lucha contra el cibercrimen que se destacan en nuestro país, y le brindan apoyo a las empresas cuando han sido víctimas de estos ataques.

De acuerdo con Microsoft, los programas informáticos ilegales representan un peligro para las organizaciones que los utilizan en tanto aumentan el riesgo de sufrir ataques de seguridad y delitos informáticos. Este flagelo le ocasiona pérdidas a la industria superiores a los 281 millones de dólares por año, aparte de sus correspondientes detrimentos fiscales.

Por todo lo expuesto, le solicito a los señores Legisladores, la aprobación del presente proyecto.-


MARIA LAURA BICCHINI
Diputada
H.C. Diputados Pcia. Bs. As.