

# POLITICAS GENERALES SEGURIDAD INFORMATICA

El tema de los riesgos de la información está de moda, y no solo por la casuística de eventos de falla y la consecuente denegación de servicios, sino porque se ha abierto un nuevo mercado para la oferta de servicios de integración, capacitación y consultoría. Sin embargo, es claro que esta oferta no necesariamente está enfocada a lo tratado, para algunos la idea es solo generar una instancia de demanda sin aclarar el objetivo final de la oferta de sus servicios.

Quando tratamos el tema de servicios orientados a los riesgos de la información, debemos identificar los objetivos de cada oferta, y para ello siempre es bueno registrarse por la norma correspondiente. En este caso, en lo que a riesgo de la información se refiere tenemos el estándar BS7799 donde está claramente establecido hacia donde deben enfocarse esos servicios, a saber, seguir los 10 mandamientos de la norma indicada.

## 1.- Planificación de la Continuidad del Servicio:

Identificar efectos críticos generados por la interrupción de servicios, por término de los procesos, y ubicación de todo aquello relativo a sus consecuencias en el negocio, en el mercado y en las personas ligadas al mismo.

## 2.- Control de los Acceso a los Servicios:

El control se refiere a la administración del acceso a la información en todo aquello relativo a autorización, prevenir pérdidas, modificaciones o el mal uso de la misma, asegurar protección de las redes de conectividad, detectar actividades no autorizado, y controlar los flujos de información sea a nivel de redes locales como redes remotas y/o móviles.

## 3.- Desarrollo y Mantención de Sistemas:

El desarrollo de los sistemas debe considerar si o si a la información, prevenir perdidas, modificaciones o el mal uso de la misma, proteger su autenticidad, su confidencialidad e integridad.

## 4.- Seguridad de Infraestructura y Ambiental:

Prevenir acceso, interferencias y/o daño a las bases físicas de la información todo ello para prevenir pérdidas, modificaciones o el mal uso de la misma.

Controles de acceso a las zonas de procesamiento y almacenamiento, el registro de los flujos físicos de la información como asimismo el seguimiento de toda aquella actividad relacionada que pudiera alterar los resultados esperados.

## 5.- Cumplimiento de Ordenanzas y Reglamentos:

Asegura el cumplimiento de normas, ordenanzas, reglamentos y/o leyes civiles u cualquier otro que regule parte o toda la infraestructura y personal relacionada con el manejo de la información.

Asimismo, cumplir con los estándares requeridos por la organización como también por las partes asociadas al negocio de manera de minimizar cuestionamientos al momento de realizar una auditoría.

#### **6.- Nivel del Personal Contratado:**

El error humano, el robo, el fraude o el mal uso de los recursos pueden eventualmente generar riesgos al manejo de la información. La disposición de servicios y elementos de seguridad, los procedimientos de validación de tareas y funciones destinadas a los usuarios quienes conscientemente deberán estar orientados a seguir pautas y reglas que aseguren el objetivo de preservar la información y sus correcto tratamiento.

Asegurar que una vez producida algún evento el personal sea capaz de resolverlos en el mínimo de tiempo y tenga la habilidad de aprender del caso.

#### **7.- Seguridad Interna de la Organización:**

Son reglas que tiene vinculación con todo aquello relativo al manejo de la información al interior de una organización, al manejo de los equipos y de los recintos donde se procese la información, y especialmente con materias de seguridad cuando se ha externalizado los procesos a servicios de terceros.

#### **8.- Administración de Redes y Computadores:**

Asegurar correcta y segura operación de equipos y sistemas asociados al manejo de la información, minimizando los riesgos de falla, protegiendo la integridad del software y de la información asociada.

Mantener integridad y disponibilidad de los procesos computacionales y de comunicaciones, asegurando el buen manejo de la información en infraestructuras de redes y dispositivos de conectividad.

Prevenir daños e interrupciones a la actividad del negocio por efectos de caídas de los sistemas, como asimismo prevenir la pérdida, daño y/o mal uso de la información por efecto de la interacción con otras organizaciones.

#### **9.- Clasificación y Control de los Activos:**

Administrar correctamente los activos físicos de la organización, llevar el registro y la mantención de equipos y sistemas, especialmente todo aquello que involucre riesgos para el manejo de la información.

#### **0.- Políticas de Seguridad:**

Establecer direcciones y soporte a todo aquello relativo a registrar, cuantificar y controlar riesgo de la información.

Definiendo con ello los objetivos corporativos y un plan marco para la seguridad de la información.

Referencias: British Standard BS7799 "Code of Practice for Information Security Management".