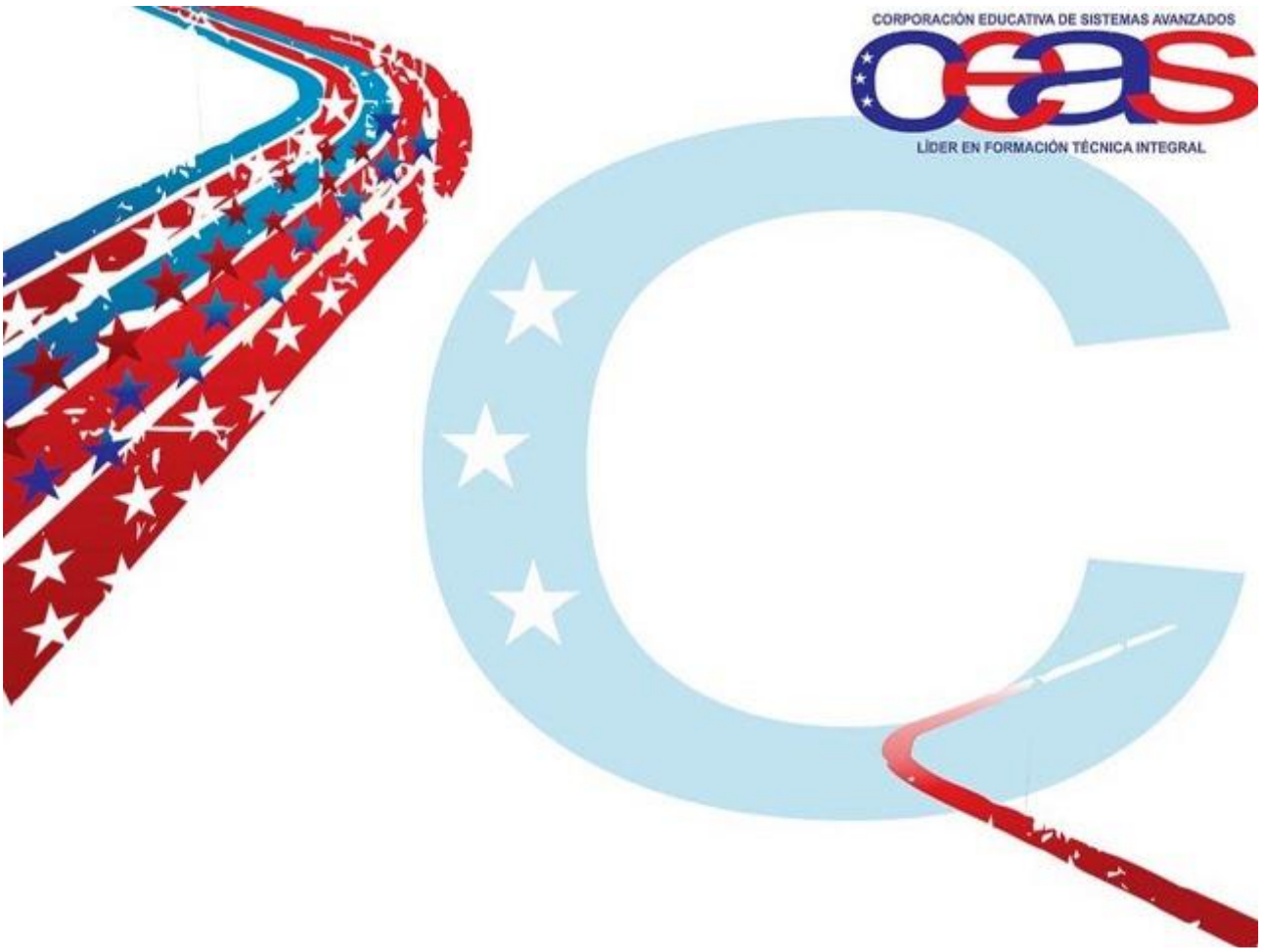
POLÍTICAS DE SEGURIDAD INFORMÁTICA



Ing. Emiro Berrio Rodríguez

Barranquilla 28 de Octubre de 2013

GENERALIDADES

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios de una organización.

ALCANCE DE LAS POLÍTICAS

Este instructivo de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y de vulnerabilidades en las dependencias de la red y su sistema información.

Pretendemos concientizar al personal de CEAS para que pueda alcanzar luego de implantar nuestro sistema de seguridad los siguientes parámetros:

- Establecer un esquema de seguridad con perfecta claridad y transparencia.
- Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Que la prestación del servicio de seguridad gane en calidad.

Todos los empleados se convierten en interventores del sistema de seguridad.

OBJETIVOS

Desarrollar un sistema de seguridad que permita planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física y lógica de los recursos informáticos, así como resguardar los activos lógicos de la empresa.

ANÁLISIS DE LAS RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "**Más Dinero Para Juguetes Del Departamento De Sistemas**".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que quienes toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la empresa.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la empresa, ellas deben responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la empresa.

RESPONSABILIDADES

Es responsabilidad del supervisor de Director de Sistemas, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, revistas internas) de los Procedimientos de Seguridad. Asimismo, es responsabilidad del supervisor inmediato capacitar a sus empleados en lo relacionado con los Procedimientos de Seguridad Informática.

BENEFICIOS DE IMPLEMENTAR POLÍTICAS DE SEGURIDAD INFORMÁTICA

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los Recursos Humanos.

DISPOSICIONES GENERALES

Articulo 1°.- El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la Empresa

Articulo 2°.- Para los efectos de este instrumento se entenderá por **Comité**
Al equipo integrado por la Presidencia y el personal administrativo (ocasionalmente) convocado para fines específicos como:

- Adquisiciones de Hardware y software
- Establecimiento de estándares
- Establecimiento de la Arquitectura tecnológica de grupo.
- Establecimiento de lineamientos para concursos de ofertas

Administración de informática
Está integrada por la Presidencia y Director de Sistemas, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Elaborar y efectuar seguimiento del plan de mantenimiento de la infraestructura informática
- Definir estrategias y objetivos a corto, mediano y largo plazo
- Mantener la arquitectura tecnológica
- Controlar la calidad del servicio brindado
- Mantener el Inventario actualizado de los recursos informáticos
- Velar por el cumplimiento de las políticas y procedimientos establecidos.

Artículo 3°.- Para los efectos de este documento, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben ser aplicadas por todo el personal de la empresa responsables del hardware y software, siendo responsabilidad del director de sistemas, vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Artículo 4°.- Las Políticas en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo de la empresa. Estas normas inciden en la adquisición y el uso de los bienes y servicios informáticos, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.

INSTALACIONES DE LOS EQUIPOS DE CÓMPUTO

Articulo 17°.- La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- La dirección de sistemas, así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Articulo 18°.- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

LINEAMIENTOS EN INFORMÁTICA: INFORMACIÓN

Articulo 19°.- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:

- Información histórica para auditorias.
- Información de interés de la Empresa
- Información de interés exclusivo de alguna área en particular.

Articulo 20°.- Los jefes de área responsables de la información contenida en los departamentos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Articulo 21°.- Se establecen tres tipos de prioridad para la información:

- Información vital para el funcionamiento del área.
- Información necesaria, pero no indispensable en el área.
- Información ocasional o eventual.

Articulo 22°.- En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

Articulo 23°.- La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

Articulo 24°.- El respaldo de la información ocasional o eventual queda a criterio del área.

Articulo 25°.- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento.
Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.

Articulo 26°.- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

Artículo 27°.- Ningún colaborador en proyectos de software y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial de la empresa tanto ahora como en el futuro.

FUNCIONAMIENTO DE LOS EQUIPOS DE CÓMPUTO

Artículo 28°.- Es obligación de la dirección de sistemas vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Artículo 29°.- Los colaboradores de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

Artículo 30°.- Por seguridad de los recursos informáticos se deben establecer seguridades:

- Físicas
- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento

Artículo 31°.- En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software personal, excepto en casos emergentes que la Dirección autorice.

PLAN DE CONTINGENCIAS INFORMÁTICAS

Artículo 32°.- La dirección de sistemas creará para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

ESTRATEGIAS INFORMÁTICAS

Articulo 33°.- La estrategia informática se consolida en el Plan Maestro de Informática y está orientada hacia los siguientes puntos:

- Plataforma de Sistemas Abiertos (Portables).
- Esquemas de operación bajo el concepto multicapas.
- Estandarización de hardware, software base, utilitarios y estructuras de datos
- Intercambio de experiencias entre Departamentos.
- Manejo de proyectos conjuntos con las diferentes áreas.
- Programa de capacitación permanente para los colaboradores de la empresa.

Artículo 34°.- Para la elaboración de los proyectos informáticos y para la presupuestación de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con los que cuente la empresa.

ACCESO FÍSICO

Artículo 35°.- Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial de la empresa

Artículo 36°.- Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

IDENTIFICADORES DE USUARIO Y CONTRASEÑAS

Artículo 37°.- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Artículo 38°.- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Artículo 39°.- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

Artículo 40°.- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Artículo 41°.- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

RESPONSABILIDADES PERSONALES

Artículo 42°.- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Artículo 43°.- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Artículo 44°.- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 45°.- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

Artículo 46°.- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

Artículo 47°.- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, placas del carro y/o las palabras como (Sexo, Amor, Love, FindeMundo, etc).

Artículo 48°.- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

Artículo 49°.- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 60 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Artículo 50°.- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Artículo 51°.- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que

contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Artículo 52°.- Los usuarios sólo podrán crear archivos que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos archivos temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Artículo 53°.- Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Artículo 54°.- Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo en Outlook)

SALIDA DE INFORMACIÓN

Artículo 55°.- Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

Artículo 56°.- Además, en la salida de datos especialmente protegidos (como son los datos de carácter personal para los que el Reglamento requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

USO APROPIADO DE LOS RECURSOS

Artículo 57°.- Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados.

Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

QUEDA PROHIBIDO

Artículo 58°.- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Artículo 59°.- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos.

Artículo 60°.- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

Artículo 61°.- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Artículo 62°.- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Artículo 63°.- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Artículo 64°.- Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

SOFTWARE

Artículo 65°.- Todo el personal que accede a los Sistemas de Información debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Artículo 66°.-Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

Artículo 67°.-También tiene prohibido borrar cualquiera de los programas instalados legalmente.

RECURSOS DE RED

De forma rigurosa, ninguna persona debe:

Artículo 68°.- Conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones (Ej. módem) que posibilite la conexión a la Red Corporativa.

Artículo 69°.- Conectarse a la Red Corporativa a través de otros medios que no sean los definidos.

Artículo 70°.- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Artículo 71°.- Intentar acceder a áreas restringidas de los Sistemas de Información o de la Red Corporativa.

Artículo 72°.- Intentar distorsionar o falsear los registros "log" de los Sistemas de Información.

Artículo 73°.- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

Artículo 74°.- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los Recursos Informáticos.

CONECTIVIDAD A INTERNET

Artículo 75°.- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los empleados tienen las mismas responsabilidades en cuanto al uso de Internet.

Artículo 76°.- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos

(Firewall) incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Artículo 77°.- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Artículo 78°.- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Artículo 79°.- En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.

ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Artículo 80°.- Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la empresa se reserva el derecho a modificar esta Política de Seguridad cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los colaboradores de la empresa.

Artículo 81°.- Es responsabilidad de cada uno de los empleados la lectura y conocimiento de la Política de Seguridad más reciente.

DISPOSICIONES TRANSITORIAS

Artículo primero.- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su difusión.

Artículo tercero.- Las disposiciones aquí descritas constarán de forma detallada en los manuales de políticas y procedimientos específicos.

Artículo cuarto.- La falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.