ÍNDICE

1 OBJETIVO
2 ALCANCE
3 DESARROLLO
4 ANEXOS

HISTÓRICO DE MODIFICACIONES

 El propósito de este documento es reflejar por escrito cuál es la Política de Seguridad de la Información de la compañía, política que cumple con la norma ISO 27001:2013.

Versión	Fecha	Propietario	Descripción
0	01/05/2015	Responsable de Calidad	Documento

1 OBJETIVO

Este procedimiento tiene por objeto definir la política de seguridad de la información de la organización.

2 ALCANCE

Afecta a toda la Organización.

3 DESARROLLO

La Dirección de la Organización ha aprobado, publicado y comunicado a todos los empleados mediante el presente sistema documental, el siguiente documento de política de seguridad de la información.

La Dirección de la Organización se compromete mediante el presente documento y todo el SGSI a poner los medios adecuados, tanto humanos, organizativos o tecnológicos para proteger la información de la Organización y la de sus clientes, y garantizar de esta forma la continuidad de la actividad de la misma en beneficio de todos sus miembros.

Inteplast tiene como objetivo estratégico la implantación de un Sistema de Gestión de Seguridad de la Información dentro de la norma ISO 27001 para alcanzar los objetivos definidos en el documento GEPG001 y el documento "*GEOC020".*

Inteplast entiende que debido a la transformación que continuamente experimenta el mercado, motivada por la evolución de las nuevas tecnologías, cada vez más existe la necesidad por parte de las empresas de externalizar sus recursos y sistemas de TI en un partner tecnológico solvente, capaz de garantizar a sus clientes un nivel adecuado de disponibilidad, integridad y confidencialidad de la información que estos le depositan, y que ello sea además contrastable.

De aquí que Inteplast haya apostado finalmente por la consecución de esta norma, a través de la cual podrá mejorar y actualizar su sistema de calidad para la seguridad de la información.

El enfoque que utiliza la Organización para gestionar la seguridad de la información está basado en la norma ISO/UNE 27001 de la cual existe documento electrónico accesible en el presente sistema documental. Su lectura permite comprender perfectamente el enfoque que la Dirección pretende dar dentro de la Organización. De todas formas se destacan los siguientes puntos:

3.1 DEFINICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, SUS OBJETIVOS GLOBALES Y SU IMPORTANCIA COMO MECANISMO QUE PERMITE COMPARTIR LA INFORMACIÓN

3.1.1 ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la Organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio elenco de amenazas para asegurar la continuidad del negocio, minimizar los daños a la Organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se caracteriza aquí como la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.

- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la Organización.

3.1.2 OBJETIVOS GLOBALES

- La Dirección de la Organización pretende disponer de una gestión de la seguridad de la información que permita a sus responsables iniciar, implantar y mantener la seguridad en la Organización.

- Persigue proporcionar una base común para desarrollar normas de seguridad dentro de la Organización y ser una práctica eficaz de la gestión de la seguridad, así como proporcionar confianza en las relaciones entre organizaciones.

- Persigue que todo lo establecido dentro del SGSI esté de acuerdo con la legislación aplicable en la materia.

3.1.3 IMPORTANCIA Y JUSTIFICACIÓN

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la Organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la Organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

3.2 EL ALCANCE DE LA POLÍTICA DE SEGURIDAD Y DEL SGSI

El alcance del SGSI abarca A TODOS los activos de negocio de la Organización. Ello implica que cualquier activo, sea del tipo que sea, está involucrado en el SGSI.

3.3 ESTABLECIMIENTO DEL OBJETIVO DE LA DIRECCIÓN COMO SOPORTE DE LOS OBJETIVOS Y PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo de la Dirección (que es el de implantar, mantener y evolucionar de forma eficaz el presente SGSI) es la base que da soporte a los objetivos y apoya y da sentido a los principios de la seguridad de la información.

3.4 BREVE EXPLICACIÓN DE LAS POLÍTICAS, PRINCIPIOS, NORMAS Y REQUISITOS DE CONFORMIDAD MÁS IMPORTANTES PARA LA ORGANIZACIÓN

- Conformidad con los requisitos legislativos y contractuales:

Es esencial para la Organización el cumplimiento de toda la legislación vigente aplicable a la misma, ya que es la base para evitar sanciones Administrativas que podrían perjudicar la continuidad de las actividades de la Organización. Asimismo lo es el cumplimiento de los compromisos contractuales con otras Organizaciones.

- Requisitos de formación en seguridad.

Es esencial para la Organización que todos sus empleados estén formados correctamente para poner en práctica todos aquellos aspectos documentados en el SGSI, sepan consultar los procedimientos y controles que les afecten y cumplan con las obligaciones propias de su perfil. Asimismo se recalcan todos aquellos aspectos de comunicación de incidencias y detección de errores de los sistemas de Información.

- Prevención y detección de virus y otro software malicioso.

Es esencial para la Organización protegerse de cualquier tipo de virus o software malicioso, por ello se han implantado sistemas de detección y destrucción de virus, de distribución corporativa y auto-actualizables. Todo ello junto con las políticas de distribución y la formación de los usuarios respecto a estos programas hace que la Organización sea mucho menos vulnerable.

- Gestión de la continuidad del negocio.

La Organización posee, mantiene, verifica y evoluciona planes de contingencia, que podrán ser aplicados en casos de interrupción del negocio por factores diversos. La Organización ha implicado en dichos planes a personal de la misma, proveedores de servicios, operadoras, etc., con el fin de garantizar la continuidad de las actividades de la Organización en caso de contingencia.

- Consecuencias de las violaciones de la política de seguridad.

Todo empleado de la Organización debe conocer la existencia de expedientes disciplinarios por violación de los compromisos adquiridos en materia de seguridad de la Información. Estos compromisos forman parte de los requisitos legales exigibles a la Organización como cumplimiento de la LOPD, por lo que la Organización derivará toda responsabilidad al infractor. De la misma forma si la Organización se considera perjudicada por una intervención de un empleado de la misma que actúe de forma desleal o maliciosa procederá a abrirle un expediente disciplinario.

Requisitos de seguridad:

Existen tres fuentes principales:

- La primera fuente procede de la valoración de los riesgos de la Organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

- La segunda fuente es el conjunto de requisitos legales, estatutarios y regulatorios que debería satisfacer la Organización, sus socios comerciales, los contratistas y los proveedores de servicios.

- La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la Organización ha desarrollado para apoyar sus operaciones.

3.5 DEFINICIÓN DE LAS RESPONSABILIDADES GENERALES Y ESPECÍFICAS EN MATERIA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, INCLUIDA LA COMUNICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD

Cada perfil dentro el SGSI posee unas responsabilidades determinadas, pero de forma genérica se pueden definir las siguientes responsabilidades generales que afectan a todos los usuarios de la Organización:

1. Se deberá guardar secreto profesional en relación a los datos de carácter personal a los que tenga acceso en virtud de su trabajo, obligación que subsistirá incluso después de finalizar sus relaciones con el titular del fichero o, en su caso, con el Responsable del mismo.

2. Los datos personales no podrán ser cedidos a terceros sin la autorización expresa del Responsable del fichero.

3. Cuando los datos estén en soporte de papel o disquetes, se guardarán en armarios o cajones debidamente cerrados con llave.

4. Cuando por razón del servicio, se hayan de facilitar datos de carácter personal a otras unidades de la propia empresa, será necesaria la autorización expresa del Responsable del fichero.

5. Comunicar, de acuerdo con el procedimiento establecido, todas las incidencias que afecten a la seguridad de los datos de carácter personal o datos de la Organización.

6. Cada usuario es responsable de la maquinaria, programa y cualquier otro equipamiento del ordenador que tenga asignado, siendo responsables de cualquier defecto resultante de la instalación de programas no autorizados, ilegales o que infecten con virus su PC. Queda rotundamente prohibido manipular el sistema operativo o desactivar protecciones de antivirus en los ordenadores personales.

7. La Organización, pone en su conocimiento que para aumentar la seguridad física, controla los accesos, asociando además a cada empleado un código numérico, del cual deberá guardar secreto.

8. Tanto el correo electrónico como el acceso a Redes Públicas (INTERNET) son herramientas que la Organización pone a disposición de sus empleados con fines exclusivamente profesionales. La Organización informa que todos los accesos a Internet y los orígenes y destinos de los correos electrónicos son registrados para su posterior análisis en caso de incidencias de seguridad.

9. Todo dispositivo personal (PDA, USB DRIVER, PORTÁTIL, etc.) propiedad de un empleado, por defecto no podrá conectarse a la red de la Organización. No obstante, y de forma excepcional, podrá conectarse a dicha red en caso de urgente necesidad y previa autorización del Responsable de Seguridad. En estos casos el equipo en cuestión conectado a la red de la Organización queda sujeto a la misma normativa en cuanto a uso y prácticas de los equipos propiedad de la Organización.

10. La Organización adopta especial cuidado para asegurar que la información no se comprometa cuando se usan dispositivos de informática móvil propiedad de la Organización tales como portátiles, agendas, calculadoras y teléfonos móviles. Por ello aplica la siguiente Política de uso de los dispositivos móviles:

    - Queda totalmente prohibida la utilización de dispositivos móviles dentro de la Organización que no hayan sido expresamente autorizados por el Responsable de Seguridad.

- Queda totalmente prohibido copiar información sobre cualquier dispositivo móvil que no sea información de agenda personal o de correo electrónico o aquella que requiera para el desarrollo de su actividad profesional y nunca sin la autorización del Responsable de Seguridad.

- Todo dispositivo móvil que deba conectarse a la red de la Organización deberá tener instalado un antivirus debidamente actualizado y un sistema de personal firewall (si accede a otras redes cuando se encuentra fuera de la Organización), así como el cliente VPN si este dispositivo debe conectarse a la Organización a través de una red pública.

- Cada usuario es responsable de los equipos de informática móvil que gestiona o utiliza, deberá protegerlos de robo, transportándolos de forma adecuada y velando por su conservación e integridad.

- Todos los dispositivos de informática móvil deberán estar protegidos por una contraseña de acceso que gestionará el propio usuario y no permitirá el acceso libre al dispositivo.

- El usuario podrá pactar con el Responsable de seguridad la salvaguarda de aquella información que crea relevante dentro de su directorio personal del servidor de Active Directory.

- Se evitará el uso de estos dispositivos en lugares públicos siempre que sea posible.

- En portátiles (ordenadores) de dirección se estudiará la aplicación de medidas de encriptación automática de información dentro del propio dispositivo. (Producto PGP) cuando existan estos portátiles.

- No se deben dejar desatendidos los dispositivos de informática móvil dentro de coches ni medios de transporte, ni en habitaciones de hotel o centros de convenciones ni en salas de reunión. Se guardarán bajo llave o se llevarán encima.

- Se ha incluido esta política durante la formación del personal que usa dispositivos de informática móvil con objeto de aumentar su percepción de los riesgos adicionales que produce esta forma de trabajo y de las medidas y controles a implantar.

3.6 DOCUMENTACIÓN QUE SUSTENTA LA POLÍTICA DE SEGURIDAD

La documentación detallada que sustenta esta política se ha desarrollado sobre un sistema de control documental accesible por toda la Organización que permite consultar todos aquellos procedimientos, documentos, medidas, registros, etc. que sean necesarios para llevar a cabo cualquier gestión de seguridad. El propio acceso a este documento ya argumenta que esta política se ha distribuido por toda la Organización, llegando hasta a todos los destinatarios en una forma que es apropiada, entendible y accesible.

4 ANEXOS

No aplica.