POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HISTORIAL DE CAMBIOS						
Revisión	**Modificación Item**	**Solicitado por Depto.**	**Descripción del cambio**	**Modificado por/fecha**	**Revisado por/fecha**	**Aprobado por/fecha**
v 1.4	---	Calidad	Actualización a google drive. Actualización normas. Adecuación política de uso por cambio de domicilio. Fusión de documentos antiguos: - GS1-04.02.01-D02 Politica del SGSI V1 - GS2-05.01.01-S01 Política de seguridad de la informacion	Alberto Esteban 25/09/2015	Alberto Esteban 25/09/2015	Alberto Esteban 25/09/2015
v 1.5	---	Calidad	Modificación de la Política de uso incluyendo nuevas directivas.	Alberto Esteban 27/10/2016	Carolina Sandoval 16/11/2016	Francisco Morén 16/11/2016
v 1.6	---	Calidad	Actualizado pie del documento con las direcciones correctas de la empresa	Alberto Esteban 2/11/2018	Alberto Esteban 2/11/2018	Francisco Morén 2/11/2018
v 1.7	---	Calidad	Actualizado comité seguridad	Alberto Esteban 10/01/2019	Alberto Esteban 10/01/2019	Francisco Morén 10/01/2019
v 1.8	---	Calidad	Cambio de formato	Bladimir Guadalupe 22/11/2019	Carolina Sandoval	Francisco Morén

ÍNDICE

1. SEGURIDAD DE LA INFORMACIÓN

1.1. Definición

La Información es un activo que, como otros activos importantes del negocio, tiene valor para Insynergy Consulting España, S.A. (en adelante ISYC) y requiere en consecuencia una protección adecuada.

Entendemos como Seguridad de la Información el conjunto de acciones y medidas destinadas a proteger y preservar la información de la Entidad y la de los medios de proceso que soportan dicha información.

La seguridad de la información protege a ésta de un amplio abanico de amenazas para:

- asegurar la continuidad del negocio.
- minimizar los daños a la organización.
- maximizar el retorno de las inversiones.

1.2. Objetivos globales

El objetivo global de la Política de Seguridad de la Información es dirigir y dar soporte a la Gestión de la Seguridad de la Información, para lo cual será necesario:

- adoptar un conjunto de medidas organizativas, técnicas, y jurídicas económicamente justificadas, y
- proporcionar a la organización los medios necesarios para su implementación efectiva, gestión eficaz y actualización periódica.

1.3. Alcance

Esta Política aplica a:

- Todo el personal de ISYC (incluidos aquellos empleados temporales, o colaboradores), así como miembros de terceros a quienes se les facilite el acceso a nuestra red, sistemas, o aplicaciones).
- Toda la información de ISYC y a los activos y servicios tales como nuestra red (correo electrónico, acceso a Internet, acceso remoto), sistemas (cortafuegos, enrutadores, servidores, y PC's), aplicaciones, bases de datos, servicios de almacenamiento y de copias de respaldo de ficheros, estén o no bajo control del IPS. Todo ello incluye los procesos de soporte a la dirección.

1.4. Importancia de la información

La gran dependencia de las actividades de la empresa respecto de los sistemas y servicios de información, y las vulnerabilidades que estos y aquellos presentan frente a las posibles amenazas sobre su seguridad, están produciendo situaciones de riesgo que las organizaciones deben manejar de manera racional y consistente, antes de que los daños sean irreparables e inasumibles.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con amenazas e inseguridades, procedentes de una amplia variedad de fuentes, tales como fraudes informáticos, espionaje, sabotaje, vandalismo, incendios, o inundaciones. Algunas de esas fuentes como virus, intrusiones, o ataques de denegación de servicio son cada vez más comunes y frecuentes, y lo que es peor más sofisticadas y dañinas.

Es pues evidente que se hace absolutamente necesario llevar a cabo determinados controles sobre aquellos riesgos que puedan poner en peligro la competitividad, la tesorería, la rentabilidad, el cumplimiento de la legalidad, la imagen comercial, y por supuesto, la continuidad del negocio y su supervivencia.

2. POLÍTICA DE SEGURIDAD

2.1. Declaración de la dirección

ISYC, desde su constitución desarrolla su actividad en torno a la Gestión de la Seguridad de la Información.

La creciente dependencia de las actividades de ISYC respecto de los sistemas y servicios de información, y las vulnerabilidades que éstos y aquéllos presentan frente a las posibles amenazas sobre la seguridad de la información, producen situaciones de riesgo que la organización debe manejar racional y consistentemente, antes de que los daños sean irreparables e inasumibles.

De lo dicho, resulta del todo evidente que ISYC plantee la necesidad ineludible de implementar y llevar a cabo determinados controles sobre aquellos activos que puedan poner en peligro la competitividad, la rentabilidad, el cumplimiento de la legalidad, la imagen comercial, y por supuesto la continuidad de nuestra actividad y la supervivencia de nuestra organización.

La política de seguridad, consecuencia de la estrategia adoptada por la Dirección de ISYC para la protección de la Información, tiene como objetivo la Implantación de un Sistema de Gestión para la Seguridad de la Información (SGSI) y la Certificación de ese SGSI en conformidad a los requisitos establecidos a través de la Norma internacional ISO-27001.

La Dirección de ISYC pretende con ello acometer un salto de calidad en la gestión de sus actividades, y al tiempo ofrecer una imagen consistente con sus servicios. Para ello proporcionará medios humanos, técnicos y económicos pertinentes, preocupándose activamente de lograr la implicación de todos los empleados de la empresa.

La Dirección de ISYC considera que la seguridad de la información constituye una de sus principales preocupaciones, y que debe estar animada por una dinámica de mejora continua, que debe difundirse por toda la organización mediante la adecuada formación, motivación y aumento de la competencia profesional.

La Dirección de ISYC considera imprescindible la implicación real de todo el personal de la empresa en la implantación, el mantenimiento, la supervisión y la mejora continua del SGSI. Además, todos y cada uno de los empleados deberán asumir la responsabilidad que les corresponde en función de su actividad dentro de la organización.

El director general reconoce que la información, entendida como elemento integrante de sus procesos de negocio, constituye uno de los activos más valiosos para la empresa.

La Dirección de ISYC a través del presente documento declara de forma expresa su firme compromiso de desarrollar, publicar, y mantener una Política de Seguridad de la Información, que facilite la protección de esos activos.

3. EL SISTEMA DE GESTIÓN

3.1. Marco del sistema de gestión

El marco y las líneas de actuación de la Política de Seguridad se proyectarán mediante el establecimiento de un Sistema de Gestión de la Seguridad de la Información.

El objetivo global del Sistema de Gestión consiste en proteger los activos de Información de ISYC de todas las amenazas, bien sean internas o externas, deliberadas o accidentales, que constituyan un riesgo no controlado para la Organización.

Definiéndolo de un modo más específico, el Sistema de Gestión deberá asegurar

El cumplimiento de:

- las normativas vigentes en materia de información y comunicaciones
- los requisitos legales sobre garantías y derechos de las personas físicas

Para ver la legislación aplicable a ISYC consultar el documento ISYC_CAL_PL_IF_IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE v 1.3

La protección de:

- la información propietaria de ISYC
- la información de la cual es depositaria por razón de sus relaciones con terceros

La operatividad de:

- los recursos materiales y tecnológicos utilizados para tratar la información
- los recursos materiales y tecnológicos necesarios para un plan de contingencia

3.2. Metodología del sistema de gestión

Desarrollar PDCA:

Planificar

- evaluar (evaluación de riesgos)
- gestionar (gestión de riesgos)

Implementar

Controlar

Realizar

- modificaciones
- mejoras

3.3. Alineamiento con el contexto

La estrategia para el Sistema de Gestión de riesgos de la organización se basa en la aplicación de una metodología apoyada y modulada por la propia experiencia, la experiencia aportada por consultoras externas y el uso de herramientas informatizadas de gestión.

3.4. Criterios de estimación del riesgo

La política del SGSI de ISYC, se basará en lo establecido en la propia norma ISO-27001 y desarrollado en el documento ISYC_CAL_SGSI_PR_ ENFOQUE DE EVALUACIÓN DE RIESGOS v 1.1.

4. POLÍTICAS, PRINCIPIOS, ESTÁNDARES Y REQUISITOS

4.1. Políticas

- Conformidad con la legislación vigente.
- Formación adecuada del personal.
- Continuidad de la gestión
- Imputabilidad en los casos de violación de la seguridad.

4.2. Normas

- ISO 27001:2014
- ISO 27002:2015

4.3. Principios

- Participación de los empleados
- Responsabilidad individual
- Eficacia de los resultados
- Prevención de incidencias

4.4. Requisitos

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada mediante dispositivos fotomecánicos o electrónicos, o hablada en conversación.

Cualquiera que sea la forma que tome, o los medios por los que se comparta o almacene deberá protegerse adecuadamente. Para entender los fines últimos de esta protección se hace necesario conocer y discernir las propiedades o atributos que califican la información.

Desde el punto de vista de la seguridad, la información se caracteriza por tres atributos:

- Confidencialidad, asegura la protección de la información sensible de acuerdo a sus diversos grados contra la divulgación no autorizada o el acceso no justificado.
- Integridad, asegura la precisión y completitud de la información, así como su validez de acuerdo con los valores y expectativas del negocio.

- Disponibilidad, asegura la accesibilidad a la información cuando ésta es requerida por los procesos de negocio, considerando las condiciones de respuesta previstas

5. RESPONSABILIDADES

5.1. Dirección

Francisco Javier Morén Sanz - CEO

Jorge Carilla

El Director es el responsable de la implementación de esta Política de Seguridad de la Información, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

5.2. Responsable SGSI (Sistema de Gestión Seguridad Información)

Alberto Esteban Vidorreta

El Responsable SGSI asumirá funciones relativas a la gestión de seguridad de los Sistemas de Información de ISYC, incluyendo todos los aspectos inherentes a los temas tratados en la presente Política

5.3. Responsable de Sistemas

Javier Marco

El Responsable de Sistemas asumirá la función de cumplir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos tecnológicos.

5.4. Comité de seguridad

Francisco Javier Morén Sanz / Jorge Carilla

Javier Marco

Alberto Esteban Vidorreta

El Comité de Seguridad procederá a revisar y proponer a la Dirección para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de Seguridad de la Información.

5.5. Propietario de activo

Los Propietarios de la Información son responsables de su clasificación en base al grado de sensibilidad y criticidad de la misma, de documentar y mantener la clasificación, y de determinar los permisos de acceso a la misma según las necesidades.

6. POLÍTICA DE USO

Dentro de este marco global de definición de la seguridad de la información, la Dirección ha decidido que se deberán dar a conocer a todos los empleados las siguientes reglas de seguridad de obligado cumplimiento y consensuadas con el Comité de Seguridad:

- Los equipos y sistemas son propiedad de ISYC y son puestos a disposición del empleado para la realización de su trabajo.
- El empleado deberá velar por el correcto uso de dichos equipos y sistemas y asegurar su integridad física.
- El empleado podrá instalar aquel software que se ajuste a sus necesidades laborales, siempre con el previo consentimiento del departamento de Sistemas.
- Queda prohibida la instalación de programa ajenos al conocimiento del Departamento de Sistemas.
- El empleado, bajo el asesoramiento del Departamento de Sistemas, deberá instalar y mantener actualizado un antivirus en su equipo asignado.
- El empleado deberá actualizar todos los parches de seguridad y actualizaciones notificadas del software alojado en su equipo.
- No se admiten modificaciones del hardware entregado sin la supervisión del Departamento de Sistemas.
- Todos los empleados deberán poseer un usuario y contraseña para acceder a los equipos de sus puestos.
- Además de la cuenta propia de cada empleado, se deberá mantener habilitada una cuenta de administrador, para poder acceder al equipo en ausencia del empleado asignado
- El empleado puede cambiar la contraseña de su propio usuario cuantas veces quiera.
- La contraseña no puede estar en blanco y no puede tener menos de 6 caracteres
- El empleado ha de guardar para su uso exclusivo su nombre de usuario y contraseña quedando prohibida su divulgación y/o la anotación de la misma en lugares visibles por terceros.
- Cuando el empleado abandone su puesto de trabajo y deje el ordenador encendido, deberá bloquear la sesión iniciada.

- El puesto de trabajo deberá en la medida de lo posible estar despejado de papeles y de soportes de almacenamiento extraíbles. Evitar el consumo de alimentos en el puesto.
- Igualmente el empleado deberá mantener una política de pantalla limpia ordenando apropiadamente sus archivos en su equipo local.
- El acceso a Internet es general para todos los empleados.
- No hay zonas de Internet restringidas y es el empleado el que hace uso de la herramienta bajo su responsabilidad.
- A todos los empleados se les proporciona una cuenta de correo electrónico. El empleado dispone de este servicio como herramienta para su trabajo y ha de usarlo exclusivamente con este fin.
- El correo electrónico es confidencial y está confidencialidad la garantiza la ley. No se accede a su contenido de ninguna forma, ni se monitoriza origen-destino de cada mensaje
- El Departamento de Sistemas se encargará de establecer sistemas adecuados para el mantenimiento e integridad de la información que se encuentra en los Servidores de ISYC.
- Si se trabaja con los datos en el disco del equipo local, es responsabilidad del propio empleado hacer las copias de seguridad.
- Los servidores se configuran para la seguridad de los datos que contienen.
- El empleado es responsable de las pérdidas de información almacenada en su equipo sin respaldo
- El empleado no abrirá mensajes de correo de desconocidos o de conocidos con asuntos en inglés o desconocidos y con ficheros adjuntos. Directamente los borrará.
- No responder nunca al correo basura (SPAM)
- No hacer caso ni reenviar mensajes de alarma en cadena tipo “Virus peligroso” o de cadena de solidaridad. Son siempre falsos.
- Todos los empleados poseen una llave para activar/desactivar la alarma del centro de trabajo de Zaragoza. El último empleado en salir del centro de trabajo, deberá cerrar con llave la cerradura principal de la puerta de entrada y activar la alarma
- En los equipos locales de trabajo, no se almacenarán datos reales de los clientes salvo que se reciba una autorización explícita y justificada para ello.
- No se imprimirán datos reales de los clientes salvo que se reciba una autorización explícita y justificada para ello.
- Se evitará imprimir documentación en la medida de lo posible.
- Ante el conocimiento de cualquier incidente de seguridad, el empleado deberá comunicarlo al comité de seguridad para que adopten las medidas correspondientes.

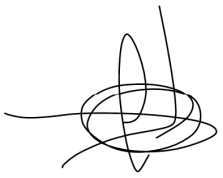
7. REFERENCIAS DOCUMENTALES

7.1. Referente para la política de seguridad

La normativa estándar inspiradora de la presente Política de Seguridad son las Normas ISO que se referencian a continuación.

- ISO 27001: 2014, tecnología de la información — Técnicas de seguridad — Sistemas de Gestión de la Seguridad de la Información (SGSI) — Requisitos
- ISO 27002: 2015, tecnología de la información — Código de buenas prácticas para la Gestión de la Seguridad de la Información.

Aprobación (firma):



Francisco Morén Sanz
CEO