



S-IT-01-00-00

Política de Seguridad

Clasificación de la Información:

| | |
|----------------------------|--|
| Nivel del Documento | Documentación General |
| Nombre del Fichero | S-IT-01-00-00-PolíticaDeSeguridad.docx |
| Tipo | DIFUSIÓN LIMITADA |
| Ámbito de Difusión | Todos los empleados |
| Responsable | Responsable de Seguridad de la Información |



CONTROL DE MODIFICACIONES

| Fecha | Versión | Descripción | Revisado | Aprobado |
|------------|---------|---|--------------------------|-----------|
| 01/10/2022 | 1.0 | Versión preliminar del documento | Responsable de seguridad | Dirección |
| 05/10/2023 | 1.1 | Renovación de documento actualizando fechas | Responsable de seguridad | Dirección |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

ÍNDICE DE CONTENIDO

| | |
|---|---|
| 1. INTRODUCCIÓN | 4 |
| 2. ALCANCE..... | 4 |
| 2.1. Empleados | 4 |
| 2.2. Sistemas de Información..... | 4 |
| 2.3. Terceras Partes | 5 |
| 3. MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA..... | 5 |
| 4. DISTRIBUCIÓN DE LA POLÍTICA..... | 6 |
| 5. SANCIONES..... | 6 |
| 6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN | 8 |

1. INTRODUCCIÓN

Los procesos de negocio de **PLASTIC7A** dependen en gran medida de los Sistemas de Información y la Información que almacenan. La Política de Seguridad tiene como misión establecer las directrices globales de Seguridad para la organización, así como proteger los activos de información.

En este documento se describen los principios donde se sostiene la Política de Seguridad de **PLASTIC7A**. Este conjunto de principios fundamentales ha sido formulado basándose en necesidades válidas de negocio, reconocimiento del valor añadido de los sistemas a proteger y una comprensión de los riesgos asociados a estos sistemas.

2. ALCANCE

2.1. Empleados

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que trabajan con Sistemas de Información. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad serán sujetos a acciones disciplinarias según se contempla en este documento.

2.2. Sistemas de Información

Esta Política afecta a todos los activos de Información de la empresa, tanto a equipos personales o servidores, redes, aplicaciones, Sistemas Operativos, procesos de la empresa que pertenecen y/o son administrados por **PLASTIC7A**.

Esta política cubre los aspectos más directamente relacionados con la responsabilidad y buen uso del personal.

2.3. Terceras Partes

La presente Política de Seguridad es de extensible conocimiento y cumplimiento para cualquier persona externa perteneciente a terceras entidades que realice cualquier tipo de tratamiento sobre la información propiedad de **PLASTIC7A**.

Asimismo, esta Política y sus procedimientos asociados serán de obligado cumplimiento para las empresas terceras proveedoras contratadas para la ejecución de servicios profesionales en los ámbitos que se consideren oportunos, en el caso de que realicen cualquier actividad que implique acceso o tratamiento a cualquier sistema o información propiedad de **PLASTIC7A** y así se definirá contractualmente.

3. MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA

El Responsable de Seguridad de la Información es el responsable de construir, mantener y publicar la Política de Seguridad de la Información, si bien, es la Dirección de **PLASTIC7A** la responsable de la aprobación de dicha Política.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido de la Política de Seguridad de la Información quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso de estas entidades por la seguridad de la información.

Periódicamente, y en todo caso no superando el plazo de un año, se revisará la vigencia y razonabilidad de la presente política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables. La dirección se compromete con la mejora continua.

4. DISTRIBUCIÓN DE LA POLÍTICA

La distribución del presente documento (Política de Seguridad de la Información), se realizará mediante correo electrónico en primera instancia y, además, quedará accesible para todo el personal en un repositorio dispuesto al efecto.

Cualquier cambio sustancial en el documento será distribuido a todos los usuarios a través de una notificación formal, enviada por correo electrónico y seguidamente será actualizado en el repositorio.

5. SANCIONES

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a **PLASTIC7A**, será sancionada de acuerdo con los mecanismos habilitados en el convenio de Empresa y en la normativa legal, contractual y corporativa vigentes.

Todos los empleados, que sean usuarios de los sistemas y servicios de información tienen la obligación de notificar al responsable correspondiente cualquier incidencia, anomalía o debilidad asociada a la seguridad de la información. Dicha comunicación se deberá realizar en el momento en que se produzca la incidencia o desde el momento en que se tenga conocimiento de la misma.

El Responsable de Seguridad, nada más comunicado el incidente de seguridad, lo catalogará y especificará su detalle, atendiendo a la gravedad del mismo, intentará solucionarlo a la mayor brevedad posible.

Se categorizan las incidencias en los siguientes términos: MUY GRAVE, GRAVE y LEVE, para facilitar la ejecución de las acciones a tomar frente a las mismas.

Se considerarán faltas leves, los incidentes con un impacto bajo, señalando las siguientes:

- Olvido del bloqueo de ordenador por parte de un usuario.
- Olvido de documentos en impresoras, fotocopiadoras, escáneres, faxes, etc. que contienen datos personales o confidenciales y no han sido retirados.

Se considerarán faltas graves, los incidentes con un impacto considerable, señalando las siguientes:

- Intentos de acceso no autorizado a recursos de la empresa.
- Degradación de servicio en los sistemas del dominio protegible.
- Acceso o lectura no autorizada de información contenida en ficheros o sistemas de información, tanto automatizados como no automatizados (soporte papel).

- Uso indebido de las cuentas y contraseñas de usuario.

Se considerarán faltas muy graves, los incidentes con un impacto extremo en los servicios de la empresa, señalando las siguientes:

- Accesos no autorizados a planta, despachos, archivos, armarios, salas, CPD's y a dependencias en las que residen sistemas de información.
- Infección masiva por virus.
- Accesos no autorizados con robo de información secreta o confidencial.
- Fugas de información confidencial.
- Copia no autorizada de la información.
- Borrado no autorizado de la información.

Las sanciones se aplicarán según convenio en función de la gravedad.

El Responsable de Seguridad determinará la raíz del incidente de seguridad, identificando a la persona o personas presuntamente responsables, velando por que el incidente de seguridad notificado no esté encubriendo un incidente de seguridad de mayor gravedad que pueda afectar a un mayor número de activos o procesos y posteriormente, estudiará la mejor forma de solucionarlo.

En caso de que estime que no tiene los conocimientos suficientes, podrá estimar necesaria la participación de otro personal de la empresa o incluso de personal ajeno a la misma especializado en la resolución de ese tipo de incidentes de seguridad.

En caso de que el sistema de información del fichero lo permita, se intentarán recoger pistas de auditoría y otras evidencias similares, consultando, entre otros, el registro de accesos al fichero en caso de estar disponible, junto a las últimas operaciones realizadas por los usuarios.

Se debe asegurar que, una vez finalizada la resolución del incidente de seguridad, la parte afectada se ha dejado con todas las medidas de seguridad que hayan sido establecidas para el mismo, realizando una descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponderle.

Y finalmente, el Responsable de Recursos Humanos analizará los incidentes de seguridad causados por el personal, en el caso de que hayan sido graves o muy graves, y decidirá el procedimiento disciplinario a aplicar en cada caso.

Todas las acciones en las que se comprometa la seguridad de **PLASTIC7A** y que no estén previstas en esta política, deberán ser revisadas por la Dirección y por el Responsable de Seguridad de la Información para dictar una resolución sujetándose al criterio de la empresa y la legislación prevista.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, **PLASTIC7A**, está altamente comprometido con mantener un servicio competitivo a través de ofrecer un modelo de negocio responsable basado en la búsqueda permanente del equilibrio económico, social y ambiental, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada.

En consecuencia, a lo anterior, **PLASTIC7A**, define los siguientes principios de aplicación a tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

- **Confidencialidad:** La información tratada por **PLASTIC7A** será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- **Integridad:** La información tratada por **PLASTIC7A** será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Disponibilidad:** La información tratada por **PLASTIC7A** estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Legalidad:** **PLASTIC7A**, garantizará el cumplimiento de toda legislación o requisito contractual que le sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

PLASTIC7A para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo éstos, uno de los activos principales de **PLASTIC7A**, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización. Para que esto no suceda, se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

1. **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
2. **Paliar** los efectos de **los incidentes** de seguridad.

3. **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
4. **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
5. **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
6. **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
7. **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
8. **Verificar** el funcionamiento de las **medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
9. **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
10. **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
11. **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de **PLASTIC7A**.
12. **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
13. **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
14. **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
15. **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.



La Dirección de **PLASTIC7A** asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas y de control necesarias para el cumplimiento de la presente Política de Seguridad de la Información. Así como, de proveer de aquellos recursos que sean necesarios para resolver con la mayor rapidez y eficacia posible, las no conformidades e incidentes de seguridad de la información que pudiesen surgir, y la puesta en funcionamiento de las medidas necesarias para que éstas no vuelvan a ocurrir.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

De igual forma, para gestionar los riesgos que afronta **PLASTIC7A** se establece un procedimiento de evaluación de riesgos formalmente definido.

Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección de **PLASTIC7A**.

APROBADO POR: GERENCIA

Nombre: Carlos González Ibáñez

Firma:

Fecha: 05/10/2023