S-IT-01-10

Política de IT

Clasificación de la Información:

Nivel del Documento	Política
Nombre del Fichero	S-IT-01-10-PoliticaIT.docx
Tipo	DIFUSIÓN ILIMITADA
Ámbito de Difusión	PÚBLICO
Responsable	Responsable de Seguridad de la Información

CONTROL DE MODIFICACIONES				
Fecha	**Versión**	**Descripción**	**Revisado**	**Aprobado**
01/10/2022	1.0	Versión inicial	Responsable de Seguridad	Dirección
05/10/2023	2.0	Revisión anual	Responsable de Seguridad	Dirección
09/07/2024	3.0	Revisión anual	Responsable de Seguridad	Dirección
19/06/2025	3.0	Revisión anual	Responsable de Seguridad	Dirección
02/07/2026	4.0	Revisión anual y cambio firmas	Responsable de Seguridad	Dirección

ÍNDICE DE CONTENIDO

Introducción

El objetivo de este documento es definir las políticas generales de IT para la gestión de cualquier acción o evento que tenga que ver con el departamento de IT, en sus diversas formas para garantizar el correcto funcionamiento de la organización siguiendo las recomendaciones de los estándares internacionales en materia de estandarización alineados a los requerimientos de las normas ISO 27001/TISAX.

1. Objeto

Establecer las líneas generales para la gestión del departamento de Tecnologías de la Información que soportan los procesos de negocio de PLASTIC7A.

2. Alcance

Todos los activos físicos y lógicos del sistema de información, dispositivos, sistemas, recursos informáticos y cualquier otro componente de la plataforma tecnológica de PLASTIC7A.

3. Gestión de Usuarios

Plastic7a define un procedimiento para la gestión de usuarios donde se cubren los siguientes puntos:

- Altas, bajas y modificaciones de usuarios y derechos de acceso lógico
- Altas, bajas y modificaciones de usuarios con acceso privilegiado
- Autorizaciones de acceso lógico
- Revisión de acceso lógico

Los usuarios y contraseñas asignadas al personal de Plastic7a son personales e intransferibles. Los requisitos de contraseñas se encuentran definidos en la política correspondiente (Ver documento S-IT-01-17-Gestion Contraseñas).
El uso de usuarios genéricos está basado en las excepciones de los operarios de plantas y están autorizadas para agilizar los sistemas de notificación de control de planta. El personal de la empresa responsables directos de los operarios son responsables de la actividad asociada a dichos usuarios. La empresa debe registrar la actividad de los usuarios, para su posterior control en caso de ocurrencia de incidentes.

La política explicada viene en el documento: S-IT-01-23-Política usuarios (altas y bajas).

4. Gestión de Activos

Plastic7a gestiona y controla sus activos a través de herramientas de software con las que obtiene toda la información necesaria de los activos. Este software se denomina LANSWEEPER. Toda la información de los activos IT se recoge y almacena en dicha aplicación. Realizándose controles periódicos de auditorías para contrastar la información almacenada.

5. Gestión de dispositivos

Plastic7a tiene definida una política de gestión de dispositivos específica que se aplica a todos los niveles para el correcto uso de los dispositivos móviles corporativos (ver documento: S-IT-01-19-Política De Uso de Dispositivos Móviles).

6. Controles de acceso físico

Plastic7a tiene definida una política de Controles de acceso físico específica (ver documento: M-MR-00-00-06 Política de seguridad física).

7. Controles de acceso lógico

Plastic7a tiene definida una política de gestión de usuarios específica y con ello los accesos lógicos a los sistemas de la organización. Está política se basa en la gestión de altas, bajas, modificaciones de los usuarios y también bien va acompañada de las acciones de buenas prácticas distribuida por la organización a todos los empleados. Para aquellos empleados capacitados a teletrabajar también hay una política específica. Los accesos al sistema están protegidos con la seguridad que aplica en cada momento, hablamos de políticas de contraseñas para aquellos accesos que lo requieran. La empresa pone a disposición de los empleados un gestor de contraseñas para almacenar las claves de acceso a las distintas aplicaciones corporativas o plataformas web. Ver documento: S-IT-01-23-04-Controles Acceso Lógicos

Otros documentos relacionados

- S-IT-01-23-Política usuarios (altas y bajas)
- S-IT-01-26-Política teletrabajo seguro
- S-IT-01-17-Gestión de contraseñas

Los sistemas de acceso lógicos esta basados en la gestión de usuarios de Active Directory (AD) y la seguridad que se aplica en cada caso. Los accesos a redes y servicios como Office 365 está integrados en la seguridad del AD. Los datos almacenados en servidores y SharePoint están sujetos a las directivas de grupo (GPO) como de las reglas de acceso mediante permisos, definidas para usuarios o grupos de usuarios.

8. Administración de redes e infraestructura

Plastic7a tiene una red de sistemas informáticos para dar servicio a toda la estructura informática de la organización. Los sistemas de red están centralizados en la ubicación denominada “Planta 1”, donde se encuentra ubicado el centro de procesamiento de datos, también denominado **CPD**. En dicha ubicación se encuentran los servidores principales, routers, switches, firewalls y demás electrónica de red necesaria junto con las entradas de comunicaciones externas que dan servicio a internet.

Dicho CPD se encuentra comunicado mediante fibra óptica con otro cuarto de comunicaciones en la “Planta 4”, el edificio de oficinas principal (HQ), donde también se encuentra toda la electrónica de red necesaria para las comunicaciones en dicha planta.

La infraestructura de red se encuentra protegida contra accesos indeseados. Solo el personal de IT está autorizado a entrar en dichas ubicaciones y terceros acompañados siempre del personal de IT.

Las instalaciones de Plastic7a tienen habilitada red Wi-Fi segura, en todas las áreas para dar servicio tanto a los equipos informáticos, donde el cableado no llega, como a otros dispositivos, como por ejemplo PDA’s o Tablets que se utilizan en la gestión del almacén y sistemas de producción. Los accesos a dichas redes wifi son administrados exclusivamente por el personal de IT, siendo confidencial las credenciales de acceso a la red de área local de la empresa.

9. Administración de servicios y aplicaciones

El departamento de IT de Platic7a se encarga de la administración de servicios informáticos y aplicaciones corporativas que ayuden al correcto desempeño de las funciones del personal de Plastic7a. La organización proporcionará todos los medios para el correcto desempeño de sus funciones laborales.

Todos los servicios y aplicaciones son monitorizados por el departamento de IT y también por terceros con los que se mantiene contratos de mantenimiento o colaboración sujetos a acuerdos de confidencialidad.

10. Requisitos de cifrado

Plastic7a tiene definida una política de cifrado específica para garantizar que se hace un uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad, autenticidad y el no repudio de la información sensible manejada por la empresa, tanto almacenada como en tránsito (ver documento: S-IT-01-20-Política cifrado).

Plastic7a dispone de una herramienta de encriptado de datos para sus equipos, especialmente los portátiles con información que podría ser considerada como sensible, tales como miembros de la dirección de la empresa. Se ha realizado despliegue de la solución de encriptación basada
en Microsoft BitLocker.

11. Gestión del cambio

Plastic7a tiene definida una política de Gestión del Cambio específica siguiendo las recomendaciones de estándares internacionales para soportar los procesos de negocio en todo lo que afecta a mantenimiento, entornos, actualizaciones, paradas de sistemas, renovaciones, etc. (ver documento: S-IT-01-21-Política de gestión del cambio).

12. Desarrollo de software

Plastic7a tiene definida una política de adquisición y desarrollo de software siguiendo las recomendaciones de estándares internacionales. El objeto es aplicar los controles de seguridad oportunos tanto en el desarrollo interno del software como en la contratación con terceros. Esta política también afecta a la adquisición de cualquier tipo de software de terceros (ver documento: S-IT-01-22-Política de adquisición y despliegue de sistemas).

Plastic7a, en SAP, tiene diferenciados los entornos de desarrollo y productivo, y por tanto también los datos usados en dichos entornos, no habiendo ninguna injerencia entre los datos de pruebas y los datos productivos. Para otros tipos de desarrollos que estén fuera de SAP, se pueden levantar servidores o servicios de forma temporal para evaluar tanto el software que se desea testear como los desarrollos que se pudiesen llevar a cabo, no obstante, esto hoy en día no sucede en Plastic7a.

13. Sistemas de seguridad y protección

Plasti7a dispone de sistemas de seguridad y protección actualizados y monitorizando en todo momento. Estos sistemas de seguridad y protección son:

- Sistemas físicos de cortafuegos **WatchGuard** con sistema de prevención de intrusiones (IPS) integrado (ver documento: S-IT-01-37-Uso Firewall corporativo).
- Sistemas antivirus y antimalware en endpoints: **WatchGuard EPDR.**
- Se disponen de sistemas de detección de intrusiones (IDS) que ayudan a detectar cualquier amenaza, hemos implementado la herramienta: **WatchGuard NDR.**
- Es de importancia relevante, mantener todos los sistemas actualizados para evitar cualquier vulnerabilidad en los sistemas a consecuencia del no mantenimiento de actualizaciones o parches de seguridad. Por ello, se lleva a cabo un plan de actualización de los principales sistemas, documentado junto en las políticas:
    - S-IT-01-22-02-Polítca de actualización de cambios de sistemas
    - S-IT-01-22-Política de adquisición y despliegue de sistemas

14. Uso de dispositivos de almacenamiento auxiliares.

Plastic7a no permite el uso de dispositivos de almacenamiento masivo ni CD/DVD. La dirección de la empresa aboga por bloquear cualquier uso de este tipo de dispositivos. El departamento de IT, mediante la aplicación de directivas de grupos (GPO), configura los equipos para que deshabiliten los dispositivos de almacenamiento masivo y de ese modo se evite su uso por parte de los usuarios. El uso de USB se permitirá en casos excepcionales debidamente justificados y siempre con la autorización del departamento de IT, una vez valorado el riesgo de su uso.

Cualquier necesidad que requiera el uso de estos dispositivos deberá ser autorizada por el departamento de IT, siempre bajo petición expresa y documentada por los canales habituales. El departamento de IT estudiará y decidirá sobre esta cuestión de forma individualizada.

15. Trasferencia segura de datos.

Plastic7a apuesta por las comunicaciones seguras con terceros. Se dispone de una política específica para tratar este tema (ver documento: S-IT-01-28-Política de ciberseguridad con terceros).

16. Almacenamiento seguro de datos.

Los datos están almacenados en servidores on-premise y cloud (SharePoint). Están sujetos a las directivas de seguridad tal como se indica en el punto 7 de control de accesos lógicos.

17. Registro y monitoreo de eventos (logs).

Plastic7a dispone de un sistema de monitorización y registros de actividades de los dispositivos la red de área local (LAN) mediante el software de monitorización Paessler PRTG, esta herramienta es adicional a los sistemas y eventos de seguridad proporcionados por otros sistemas de la red como pueden ser el propio visor de eventos de los servidores, el servidor de syslog (Graylog) o el cortafuegos.

18. Gestión de vulnerabilidades.

Una vulnerabilidad es una debilidad o un error de diseño o implementación que puede desembocar en un evento que comprometa la seguridad de un dispositivo, sistema operativo, red, programa o de un protocolo envuelto en cualquiera de los anteriores. No debe confundirse una vulnerabilidad con un incidente de seguridad.

Plastica7a ya dispone de una política para la gestión de incidentes, documento: S-IT-01-16-Gestión de incidentes. Por ello podemos recoger los diferentes tipos de incidentes relacionados con vulnerabilidades identificadas o conocidas. Estos casos de incidentes provocados por vulnerabilidades serian:

- Intentos de intrusión:
  - Explotación de vulnerabilidades conocidas: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (buffer overflow, XSS, backdoor…).
  - Múltiples intentos de acceso con vulneración de credenciales (brute force, password cracking…).
  - Ataque desconocido empleando exploit
  - Compromiso de aplicaciones: Vulnerabilidades de software.

- Disponibilidad:
  - DoS/DDoS mediante envío de peticiones masivas para ralentizar su funcionamiento o interrumpir el servicio.

- Sistemas vulnerables:
  - Servicios accesibles que pueden presentar criptografía débil.
  - Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para sobre cargar una red o servidor (DNS).
  - Otras causas: mala configuración, sistemas desactualizados, falta de antivirus, falta de firewall, etc.

Acciones no permitidas en la búsqueda de vulnerabilidades:

- Usar ingeniería social.
- Comprometer el sistema y mantener el acceso a este de manera persistente.
- Alterar datos.
- Usar malware.
- Utilizar la vulnerabilidad más allá de la demostración de su existencia.
- Uso de la fuerza bruta.
- Compartir con terceros.
- Realizar ataques DoS o DDoS.

18.1. Tratamiento de vulnerabilidades

Plastic7a recibe una notificación de vulnerabilidad, por lo medios habilitados del mismo modo que indica la Política de Gestión de Incidente. El primer paso es comprobar si se trata de una nueva vulnerabilidad en algún producto, o de un incidente de usuario final.
En el primer supuesto, cuando se trata de una nueva vulnerabilidad en algún producto, el equipo IT, gestiona esas vulnerabilidades no conocidas aún por parte del fabricante del activo afectado, además coordina la comunicación entre el investigador y el dueño del producto afectado, realiza la divulgación pública de la nueva vulnerabilidad y la documenta a las partes interesadas.

Para la segunda opción, en el caso de un incidente de usuario final, el equipo de gestión de incidentes de PLASTIC7A sería el encargado de realizar el *triaje* y clasificación del incidente, notificar a los usuarios interesados/afectados y compartir los detalles técnicos y soluciones.

19. Planes de contingencia y recuperación de desastres.

Plastica7a ha desarrollado el documento: S-IT-01-31-Analisis de Impacto del Negocio (BIA), a partir de este análisis, se ha desarrollado el documento: S-IT-01-30-Plan de Recuperación de Desastres (DRP). Este documento contempla los planes de contingencia y proceso de recuperación que la empresa ha definido como resultado de análisis previo aprobado por la dirección.

20. Copias de seguridad y redundancia.

Plastic7a ha desarrollado documento sobre la política de backups donde se detalla cómo, dónde, con qué periodicidad y durante cuánto tiempo se almacenan dichas copias de seguridad (ver documento: S-IT-01-27-Política de backups).

21. Prevención de fuga de datos.

El Data Loss Prevention (DLP) es un conjunto de políticas y aplicaciones software cuyo objetivo es monitorizar la información del sistema y evitar la posibilidad de perder o violar datos por diversos motivos. La prevención de pérdida de datos sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la red corporativa. El término describe productos de software que ayudan a un administrador de redes a controlar los datos que los usuarios pueden transferir. Los productos de DLP usan reglas de negocio para clasificar y proteger la información confidencial y crítica, para que los usuarios no autorizados no puedan intercambiar datos de manera accidental o malintencionada, cosa que podría poner en riesgo a la organización.

Plastic7a está adoptando la DLP a causa de las amenazas internas y las rigurosas leyes de privacidad de datos, muchas de las cuales contienen requisitos muy exigentes para protección o acceso a los datos. Además de monitorizar y controlar las actividades en los puntos de contacto, algunas herramientas de DLP se pueden usar para filtrar corrientes de datos en la red corporativa y para proteger datos en movimiento. Por ello, tenemos una guía de buenas prácticas básicas, que se distribuye en plan de acogida de los empleados, con los siguientes puntos:

- Priorizar datos. No todos los datos son igual de críticos. Decidir cuales causarían los problemas más graves en caso de robarse.

Clasificación de datos. Asociar una clasificación por contexto. Aplicar etiquetas de clasificación persistente y hacer seguimiento (ver S-IT-01-15-Clasificación de la documentación).

- Monitorizar los datos en movimiento. Obtener visibilidad de lo que está ocurriendo con los datos sensibles y determinar alcance de los problemas para abordar una estrategia.

- Comunicar y desarrollar controles. Establecer controles con la dirección para reducir el riesgo de pérdida de datos. Los controles pueden abarcar comportamientos comunes que pueden considerarse de riesgo y madurarlos para afinarlo para reducir riesgos específicos.
- Formación de empleados y orientación continua. A veces los empleados no suelen darse cuenta de que sus acciones pueden redundar en pérdidas de datos. Hay que instruirlos. Hay soluciones avanzadas que ofrecen advertencias sobre violación de políticas.
- Implementación de controles refinados. Clasificar los datos, inicialmente trabajar con un subconjunto de datos críticos y con el tiempo hacerlo extensivo al resto de datos para reducir el riesgo.

Plastic7a está implementado medidas para prevenir la perdida de datos basadas en:

- Correo electrónico: Proteger contra el phishing y la ingeniería social mediante la detección de mensajes entrantes y salientes.
- Red: Monitorizar la red para detectar cualquier anomalía.
- Cloud: Los datos en SharePoint, están monitorizados y protegidos.

APROBADO POR: LA DIRECCIÓN DE PLASTIC7A
Este documento ha sido aprobado formalmente por la Dirección General de PLASTIC7A con fecha 02/07/2026. La versión original firmada electrónicamente se conserva en el repositorio documental del SGSI. La versión publicada en la web corporativa es una copia informativa. **Fecha: 02/07/2026**