POLÍTICA DE SEGURIDAD Y BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS

TOPOGRAFIA MALLORCA S.L.

POLÍTICA DE SEGURIDAD Y BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS DE TOPOGRAFIA MALLORCA S.L.

INTRODUCCIÓN

Este documento expone la Política de Seguridad y Buenas Prácticas en protección de datos de TOPOGRAFIA MALLORCA S.L. con CIF B57648057

Los avances tecnológicos en Internet, las redes, los dispositivos y la computación en la nube; junto a los servicios derivados de éstos como el comercio electrónico, la administración electrónica, los blogs, las redes sociales y las herramientas de colaboración, están transformando la forma de hacer negocios.

Es fundamental para la organización gestionar adecuadamente la infraestructura tecnológica sobre la cual se sostiene la información de la empresa: servidores, dispositivos de red, aplicaciones de gestión, sistemas de gestión empresarial, etc. El aumento de estos recursos tecnológicos ha desembocado en que su gestión sea considerada como uno de los pilares fundamentales, debido, sobre todo, a la dependencia que el negocio tiene de las infraestructuras tecnológicas.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La dirección de la empresa, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

DEFINICIONES

Sistema de Información:

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Gestión de riesgos:

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Sistema de Gestión de Seguridad de la Información (SGSI):

Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Disponibilidad:

Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.

Integridad:

La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

Confidencialidad:

La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

Autenticidad:

Se debe asegurarla identidad u origen de la información.

Trazabilidad:

Se debe asegurar para ciertos datos quién hizo qué y en qué momento.

ALCANCE Y OBJETIVOS

La presente Política de Seguridad y Buenas Prácticas en protección de datos es proteger los activos de información de la empresa, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la empresa.

El personal sujeto a esta Política incluye a todas las personas con acceso a la información, independientemente del soporte automatizado o no en el que se encuentre ésta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la empresa.

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

• Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

• Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

• Principio de disponibilidad y continuidad: se debe garantiza un nivel de disponibilidad en los sistemas de información y se debe dotar los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

• Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

• Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegure que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

• Principio de concienciación y formación: se deben articular iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información.

• Principio de prevención: se deben desarrollar planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

• Principio de detección y respuesta: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.

CLASIFICACIÓN DE LAS AMENAZAS

Las nuevas tecnologías han impactado de forma positiva en nuestras empresas, pero, al igual que cuando éstas no existían, los riesgos a los que está expuesta la información se mantienen. Imaginemos, por ejemplo, un libro de contabilidad. Existe el mismo riesgo de pérdida de datos, extravío, robo, etc. para un libro «clásico» en papel que no custodiamos debidamente, como el que se encuentra en un fichero de datos dentro de nuestro ordenador portátil. Los medios cambian, pero los riesgos continúan. Siguiendo una serie de medidas básicas de seguridad podemos reducirlos.

La organización debe tener presente las amenazas a las que está expuesta y la forma en la que se puede hacerles frente.

La empresa tiene información que hay que proteger frente a una serie de amenazas. Básicamente, podemos distinguir entre amenazas externas e internas, y en ambos casos, pueden ser intencionadas o accidentales.

Amenazas externas intencionadas

Espionaje, sabotaje, vandalismo, robo de información confidencial son algunas de las amenazas externas a las que se puede enfrentar la empresa.

Amenazas externas accidentales.

En muchas ocasiones las amenazas son involuntarias o resultantes de desastres naturales, que pueden derivar en muchos casos en inundaciones o incendios.

Amenazas internas intencionadas.

Una de las amenazas que deben resolver los departamentos de informática es el propio personal de la organización, como podría ser un empleado con acceso a los recursos de la organización que sabe que va a ser despedido.

Amenazas internas accidentales

Comprenden las malas prácticas por parte de un empleado, sin tener una mala intención, por ejemplo insertar un USB infectado en un ordenador corporativo.

BUENAS PRÁCTICAS

Una vez conocidas las amenazas que pueden afectar a los activos de información de la empresa, se deben aplicar una serie de medidas de seguridad básicas. Además de la aplicación de las medidas organizativas y de cumplimiento legal, la empresa aplicará medidas para:

- La gestión, identificación y clasificación de los soportes;
- La seguridad de las operaciones:
    - Control de acceso a sistemas y aplicaciones
    - Gestión segura de las contraseñas
    - Control para el uso correcto de los correos electrónicos
    - Análisis de las capacidades de los Servidores
    - Gestión y control de los elementos de protección de los equipos
    - Gestión de copias de Seguridad y borrado de datos.

MEDIDAS Y REQUISITOS DE SEGURIDAD

Las medidas y requisitos de seguridad de la empresa tienen por objetivo identificar y gestionar los soportes activos de la organización y definir las responsabilidades de protección sobre los mismos. Esto incluye desde la realización de un inventario, hasta la definición de los usos aceptables.

GESTIÓN, IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS SOPORTES

Identificación de los Activos

La gestión de los activos de una organización es uno de los aspectos más complicados y a la vez más claves en un departamento de informática. Son muchos los activos que gestiona una empresa (ordenadores personales, teléfonos móviles corporativos, tabletas, portátiles, proyectores, servidores, aplicaciones software, monitores, periféricos, etc.). Por ello es necesario que se realice y se mantenga actualizado un inventario en el que los activos se encuentren clasificados y gestionados de la manera correcta.

Gestión y clasificación de soportes

La gestión de soportes persigue evitar que se revele, modifique, elimine o destruya de forma no autorizada la información almacenada en los mismos.Se debe prestar especial atención los soportes móviles usados en la organización. Estos dispositivos pueden almacenar información confidencial de la empresa y tienen una alta probabilidad de pérdida o de sufrir un robo.

Por ello deberán estar etiquetados e inventariados indicando como mínimo:

- tipo y marca del dispositivo
- persona asignada al dispositivo
- número de serie
- tipo de uso
- ubicación

Para ello TOPOGRAFIA MALLORCA S.L. describe los medios con los que cuenta la organización para el tratamiento de los datos:

Relación de ordenadores y soportes electrónicos:

ORDENADOR DE SOBREMESA, con marca/modelo DELL, serie/identificación del dispositivo -, con el sistemas operativo WINDOWS 10 PRO, con el software usado MICROSOFT OFFICE, CORREO ELECTRÓNICO.

ORDENADOR DE SOBREMESA, con marca/modelo MSI, serie/identificación del dispositivo -, con el sistemas operativo WINDOWS 10 PRO, con el software usado MICROSOFT OFFICE, CORREO ELECTRÓNICO.

SERVIDOR (NAS), con marca/modelo -, serie/identificación del dispositivo -, con el sistemas operativo -, con el software usado -.

ORDENADOR PORTÁTIL - PETER, con marca/modelo MSI, serie/identificación del dispositivo -, con el sistemas operativo WINDOWS 10 PRO, con el software usado MICROSOFT OFFICE, CORREO ELECTRÓNICO.

ORDENADOR PORTÁTIL, con marca/modelo -, serie/identificación del dispositivo -, con el sistemas operativo -, con el software usado -.

Relación de soportes en papel:

DOCUMENTACIÓN EN SOPORTE PAPEL, y a su vez ubicado dentro del centro en ARMARIO CERRADO CON LLAVE EN INTERIOR DE CENTRO DE TRABAJO.

SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones abarca las actividades encaminadas a asegurar el correcto funcionamiento del equipamiento donde se realiza el tratamiento de la información, desde su instalación y puesta en marcha, pasando por su actualización y protección ante software malicioso y la realización de copias para evitar la pérdida de datos, hasta la monitorización y el registro de las incidencias.

Control de acceso a sistemas y aplicaciones

Para prevenir el acceso no autorizado a los sistemas y aplicaciones se debe restringir el acceso a los mismos de acuerdo con una política definida por la organización. Esta política limitará el acceso a los recursos, evitando accesos no autorizados y garantizando el acceso de los usuarios autorizados. Estas políticas abarcan el control del acceso físico y lógico.

El control del acceso físico evitará la pérdida, daño, robo o alteración de los activos y la interrupción de las operaciones. Algunas de estas medidas son la separación de áreas, los tornos de acceso, etc.

En cuanto al acceso lógico se han de implantar, cuando sean necesarios, procedimientos de acceso seguro de inicio de sesión (autenticación), y sistemas interactivos para establecer y cambiar con frecuencia las contraseñas de forma que sean seguras y robustas.

Para ello TOPOGRAFIA MALLORCA S.L. aplica las siguientes medidas de control de acceso a los datos:

- Existen restricciones de acceso a los datos:
    - Las personas no autorizadas no pueden tener acceso a los equipos.
    - Todos los usuarios de los equipos cuentan con claves de acceso propias, no compartidas, que se modifican de forma periódica.
- Medidas de protección de datos de categorías especiales
    - No aplica medidas de protección de datos de categorías especiales
- Dispositivos con acceso remoto integrado
    - Se proporciona acceso remoto al equipo a personas autorizadas y con contraseñas de acceso (acceso mediante conexiones seguras).

Gestión segura de las contraseñas

Es importante que la empresa realice una correcta gestión de las contraseñas que se usan para acceder a los distintos servicios de la organización, especialmente cuando se trate de usuarios de administración de los equipos. Se debe establecer una política segura en la creación, mantenimiento y cambio de contraseñas, con el fin de mantener la seguridad y la privacidad de la información.

Se debe seguir una serie de hábitos adecuados para la gestión de las claves:

- Que sean robustas, es decir, que tengan más de ocho caracteres y aparezcan mayúsculas, minúsculas, símbolos especiales y números.
- Evitar contraseñas fáciles como nombres, palabras o expresiones que coincida con el propio usuario, que estén en blanco o que coincida con contraseñas anteriores que han sido utilizadas por el usuario.
- Las contraseñas han de caducar al menos cada 12 meses.
- Utilizar un gestor de claves para almacenarlas y realizar copias de seguridad regulares.

Control para el uso correcto del correo electrónico

En el momento de utilizar el sistema de correo electrónico profesional, se debe respetar lo que se establece en las normas de uso del correo electrónico establecidas por la empresa. Más allá de esta cuestión, conviene tener presentes algunas buenas prácticas para utilizar esta herramienta de una forma respetuosa con la privacidad de las personas

Para ello TOPOGRAFIA MALLORCA S.L. aplica las siguientes medidas de control para el uso correcto del correo electrónico:

- Se Instala y activa aplicaciones antimalware y filtros antispam tanto en el servidor como en los clientes de correo.
- Se usan contraseñas seguras para acceder al correo electrónico.
- Se Identifican a los remitentes antes de abrir un correo electrónico y si se sospecha que ha sido suplantada la identidad se contacta con el remitente por otro medio para confirmarlo.

Análisis de las capacidades de los Servidores

Periódicamente se debe realizar un análisis de capacidad de los servidores y dispositivos que tiene la organización. Para ello, muchos equipos disponen de funcionalidades básicas de monitorización, y en el mercado hay herramientas que permiten realizar un seguimiento adecuado.

Los recursos que se disponen en un servidor son limitados, por lo que además de monitorizarlos correctamente, es necesario realizar un análisis de recursos y necesidades futuras previendo de esta forma evitar que los equipos y sistemas se saturen, con consecuencias indeseadas.

Para ello TOPOGRAFIA MALLORCA S.L. aplica las siguientes medidas de seguridad para analizar las capacidades y el uso correcto de los Servidores:

- Los servidores se encuentran ubicados en un país de la Unión Europea o en países que ofrecen garantías de protección de datos

• El servidor recoge detalles de las actividades de tratamiento (controles de acceso, quién accede, cómo, cuándo, dónde, etc.)

• El servidor permite conocer en todo momento la ubicación de los datos.

• El servidor permite disponer en cualquier momento de los datos y facilita la portabilidad.

• El proveedor ha informado de los niveles de seguridad garantizados y los procedimientos de auditoría que tiene previstos.

• Existe contrato de confidencialidad suscrito con el proveedor (recuerde la importancia de registrar al proveedor como encargado del tratamiento.

Gestión y control de los elementos de protección de los equipos

Se debe verificar que todos los equipos se encuentren en el sistema de gestión del antivirus, cortafuegos y antispam y que se realicen correctamente los análisis periódicos de los equipos, para evitar infecciones.

Hoy en día existen multitud de herramientas que facilitan la ejecución de este trabajo, por lo que un mantenimiento adecuado, no resulta complicado. Se debe tener una buena gestión acompañado de una programación de revisiones periódicas para corroborar que todo se realiza correctamente.

Para ello TOPOGRAFIA MALLORCA S.L. aplica los siguientes elementos de protección de los equipos:

• Antivirus.

Seguridad del tratamiento en papel

TOPOGRAFIA MALLORCA S.L. aplica las siguientes medidas de seguridad para tratamiento en papel:

• la ubicación del soporte impide el acceso a personas no autorizadas (bajo llave, etc.)

• la ubicación y el tipo del soporte garantiza la integridad de los datos, permitiendo su conservación en condiciones ambientales adecuadas.

• la ubicación del soporte garantiza la disponibilidad de los datos en cualquier momento.

Gestión de copias de Seguridad y borrado de datos.

Una de las medidas de seguridad más importantes es la implantación de un sistema de copias de seguridad que garantice la recuperación de los datos y la continuidad del negocio en caso de que se materialice alguna amenaza que afecte a los mismos.

Se debe definir e implantar diferentes procesos para la gestión de las copias de seguridad, incluyendo pruebas de restauración periódica para garantizar que se realizan adecuadamente.
Además, es importante adoptar medidas de seguridad adicionales para proteger las copias contra pérdida, daño o acceso no autorizado:

• Almacenar las copias en medios físicos (cintas, DVD, discos duros externos)

• Almacenar las copias en sitios cerrados seguros, en una ubicación distinta del original para poder restaurar la información en caso de desastre.

• Restringir el acceso a las ubicaciones donde se encuentran las copias exclusivamente a las personas autorizadas.

También existe la opción, como alternativa al medio físico, de utilizar la nube (servicios de copias de seguridad online) como lugar de almacenamiento o replicación de las copias de seguridad de la organización.

TOPOGRAFIA MALLORCA S.L. realiza copias de seguridad.

La periodicidad con la que se realizan las copias de seguridad es DIARAMENTE

Los soportes en los que se realizan las copias de seguridad, no pudiendo ser los mismos empleados para el tratamiento de los datos, son SERVIDOR (NAS)

Se aplican las mismas medidas de seguridad a los soportes en los que se realizan las copias de seguridad.

Se restringe el acceso a las ubicaciones donde se encuentran las copias de seguridad exclusivamente a las personas autorizadas.

Borrado de datos

TOPOGRAFIA MALLORCA S.L. procede a la destrucción segura de la información una vez terminada su vida útil.

Mediante el siguiente procedimiento de borrado de datos DESTRUCTORA O TRITURADORA (PAPEL) Y BORRADO DE CARPETA DE DESCARGAS Y PAPELERA RECICLAJE (DIGITAL)