tower

POLÍTICA INTERNA

Seguridad de la Información

POL-02

ISO 27001
Sistema de gestión de seguridad de la información

Elaborado por Héctor Oliva López

Aprobado por Comité de Seguridad

Control de versiones

Versión	Fecha	Autor	Cambios
1.0	23/03/2023	Rubén Navío	Revisión Inicial
2.0	21/03/2024	Hector Oliva	Cambio y adaptación de termino

Revisión

Responsable	Última revisión	Siguiente revisión	Comentarios

Control de cambios

Versión	Fecha	Resumen de los cambios producidos
2.0	21/03/2024	Se cambia el etiquetado del documento, pasa a ser Confidencial

Índice

Objeto

Tower Consultores depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el ENS.

Referencias y anexos

La implantación de este procedimiento requiere la consideración de la siguiente documentación:

- **Política de Seguridad de la Información.**
- **Normativa de Seguridad.**
- **UNE-ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.**
- **UNE-ISO/IEC 27002 Código de Prácticas para los Controles de la Seguridad de la Información.**
- **Documentos y guías del Centro Criptológico Nacional (CCN-STIC) referidos al ENS.**

Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Alcance

Esta política se aplica a todos los sistemas TIC de Tower Consultores y a todos los miembros de la organización, sin excepciones.

Misión

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, Tower Consultores, está altamente comprometido con mantener la Promoción de proyectos de investigación, desarrollo tecnológico e innovación, en un entorno de calidad, 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, Tower Consultores, define los siguientes principios de aplicación para tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

La Dirección de Tower Consultores, entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de los servicios de la organización, y, por tanto, soporta los siguientes objetivos y principios:

- Implementar el valor de la Seguridad de la Información en el conjunto de la Organización.
- Contribuir, todas y cada una de las personas de Tower Consultores, a la protección de la Seguridad de la Información.
- Preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información, con el objetivo de garantizar que se cumplan los requisitos legales, normativos, y de nuestros clientes, relativos a la seguridad de la información; y de forma específica en lo que respecta a datos de carácter personal:

  - Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado (Licitud, lealtad y transparencia).

  - Serán, recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (Limitación de la finalidad)

- Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (Minimización de datos).

- Los datos deberán ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (Exactitud).

- Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (Limitación del plazo de conservación)

- Tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (Integridad y confidencialidad).

  - Proteger los activos de la información de Tower Consultores de amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad del servicio ofrecido a nuestros clientes y la seguridad de la información.
  - Establecer un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por Tower Consultores.
  - Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.
  - Asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.
  - Extender nuestro compromiso con la seguridad de la información a nuestro personal trabajador y proveedores.
  - Mejorar continuamente la seguridad mediante el establecimiento y seguimiento periódico de objetivos de seguridad de la información.

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.

Marco Normativo

La gerencia de Tower Consultores se asegura de que la documentación de origen externo que resulta de interés para el funcionamiento de la empresa es conocida por los empleados de la empresa que lo necesitan y es mantenida actualizada y disponible en todo momento.

Para ello se utilizan los medios definidos en este documento y los procedimientos que lo desarrollan.

En cuanto a normas aplicadas para formalizar los diferentes procedimientos de Seguridad establecidos se han seguido los criterios de las siguientes normas internacionales:

- Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. **UNE-ISO/IEC 27001**
- Tecnología de la información. Técnicas de seguridad. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. **UNE-ISO/IEC 27002**
- Exigencias de partes interesadas
- De forma adicional se crea el **Registro Normativa aplicable** para nutrir de toda la información, enlaces de interés e información relacionada con la Normativa aplicada.

Nombramientos y organización de responsables

La dirección de Tower Consultores se encarga de realizar unos nombramientos para designar los roles y responsabilidades, así como los comités necesarios, para velar por el cumplimiento de esta política.

Esta documentación estará accesible para todas las partes interesadas y el personal interno a la organización.

Roles: Funciones y responsabilidades

En el documento interno REG-02_Roles y responsabilidades Tower Consultores_v2.0 se recogen con detalle todos los roles y responsabilidades de la organización.

Procedimientos de designación

El responsable de Seguridad de la Información será nombrado por Dirección a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo con la Ley 11/2007 designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

Datos de carácter personal

Tower Consultores trata datos de carácter personal. El drive corporativo (ubicado en la UE), al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de Tower Consultores se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Clasificación de la información

Tower consultores cuenta con un sistema interno de clasificación de la información en función de su criticidad. Aquella información sensible con un nivel de criticidad relevante es cifrada y tratada antes de ser enviada o salir de la organización.

Este sistema esta descrito y procedimentado en el sistema interno de la organización.

Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

A causa de la protección de datos personales puede ser necesario aumentar las medidas propuestas por el propio ENS.

Desarrollo de la política de seguridad de la información

Esta política se desarrollará por medio de normativa de seguridad que afrontará aspectos específicos en la operativa de los usuarios de IT de la organización.

La política de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La política de seguridad estará disponible en https://towerconsultores.com, en la página principal del repositorio de datos "SharePoint" de la empresa y que está disponible en la intranet corporativa alojada en el servidor interno principal de la empresa.

https://towerconsultoressl.sharepoint.com/:w:/r/documentacion/ESQUEMA NACIONAL DE SEGURIDAD/ENS - COMITÉ SEGURIDAD/OFICIALES/POLITICAS/POL_01 Política de seguridad de la información_v1.0.docx?d=w94987b9dfc14439eb23e2ac820ff67b6&csf=1&web=1&e=n96vcv

Obligaciones del personal

Todos los miembros de Tower Consultores tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Tower Consultores atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Terceras partes

Cuando Tower Consultores preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Tower Consultores utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Firma por la dirección

Madrid a 21 de marzo del 2024