1. Aprobación y entrada en vigor.

Texto aprobado el día 29 de Julio de 2022 por la Dirección de ASTIBOT INGENIERÍA INFORMÁTICA, ROBÓTICA Y DOMÓTICA S.L. (ASTIBOT).

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. Introducción

ASTIBOT depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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 a 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 ASTIBOT debe 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.

ASTIBOT debe 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 el desarrollo de todos los proyectos y servicios prestados por la organización.

ASTIBOT deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS, con la aplicación de las medidas que se toman a continuación.

2.1. Prevención

Las diferentes áreas o departamentos de ASTIBOT 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

2.2. 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 según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. 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.

2.3. Respuesta

En ASTIBOT se debe:

- 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 clientes y los Equipos de Respuesta a Emergencias (CERT) que puedan ser necesarios.

2.4. Recuperación

Para garantizar la disponibilidad de aquellos servicios que pudieran considerarse críticos, ASTIBOT debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. Alcance

Esta Política se aplicará a los sistemas de información de ASTIBOT y a todos los miembros de la organización implicados en servicios y proyectos destinados al sector público y privado que requieran la aplicación del ENS.

Todos los miembros tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

4. Misión

ASTIBOT INGENIERÍA INFORMÁTICA, ROBÓTICA Y DOMÓTICA S.L. (ASTIBOT) es una empresa dedicada al desarrollo de software a través de la aplicación de la tecnología a su alcance.

ASTIBOT, debido a su especialización, se depende de los sistemas de tecnologías de información y comunicaciones (TIC) para alcanzar sus objetivos asumiendo el compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Los sistemas de información deben ser administrados con diligencia y tomando las medidas más adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad y confidencialidad de la información tratada y de los servicios prestados. 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 ASTIBOT debe 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.
ASTIBOT debe 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 y en la solicitud de ofertas para proyectos de TIC.

ASTIBOT debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS (Artículo 7. Prevención, reacción y recuperación. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Actualizado el 04/11/2015).

5. Objetivos

La Dirección de ASTIBOT establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

6. Marco normativo

El marco normativo en que se desarrollan las actividades de ASTIBOT y particularmente la prestación de sus servicios están compuestos por las siguientes normas:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado por Real Decreto 951/2015, de 23 de octubre.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de Febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

También forman parte del marco normativo las restantes normas aplicables para la administración electrónica en ASTIBOT derivadas de las anteriores y que están comprendidas dentro del ámbito de aplicación de la presente Política.

7. Principios básicos

Toda la actividad relacionada con el uso de los activos de información y el tratamiento de datos personales se regirá por los siguientes principios fundamentales:

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de ASTIBOT, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

- Responsabilidad determinada: en los sistemas TIC se determinará el Responsable de la Información y del Servicio, que determina los requisitos de seguridad de la información y de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema de información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de Riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

- Proporcionalidad: el establecimiento de medidas de prevención, detección, reacción y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados. Así mismo, la estrategia de protección estará constituida con múltiples líneas de capas de seguridad de forma que cuando una capa falle podamos ganar tiempo para una reacción adecuada, reducir la probabilidad de compromiso del sistema y minimizar el impacto final.

- Principio de profesionalidad: la seguridad de los sistemas estará implantada, atendida, revisada y auditada por personal cualificado y formado, que participará en todas las fases del ciclo de vida de los sistemas.

- Mejora continua: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

- Seguridad por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

8. Organización de la seguridad

ASTIBOT, teniendo en cuenta lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica y las pautas establecidas en la Guía CCN-STIC-801 “Responsabilidades y Funciones en el ENS”, para organizar la seguridad de la información emprenderá las siguientes acciones:

1. Designará roles de seguridad: Responsables de la Información y de los Servicios, Responsable de la Seguridad y Responsable del Sistema haciéndolas constar en su organigrama de empresa.

2. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información que será denominado Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

8.1. Comité de seguridad de la información: funciones y responsabilidades

El Comité de Seguridad de la Información está formado por

- Responsable de la Información y de Servicio
- Responsable de Seguridad
- Responsable de Sistema

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité que actuará en el ámbito del cumplimiento de las medidas a las que se refiere el Real Decreto 3/2010, de 8 de enero.

Le corresponden las siguientes funciones:

a) Estar permanentemente informado de la normativa que regula el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
b) Velar por el cumplimiento de las normativas legales, así como alinear las actividades de la organización con los objetivos de seguridad de la información.
c) Promover la divulgación de esta Política de Seguridad de la Información y revisarla periódicamente.
d) Velar por la disponibilidad de recursos necesarios para el desarrollo de esta Política de Seguridad de la Información y el mantenimiento de la Seguridad de la Información.
e) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
f) Coordinar los esfuerzos de las diferentes áreas y responsables en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
g) Atender las inquietudes, en materia de Seguridad de la Información, de ASTIBOT y de los diferentes departamentos, informando regularmente del estado de la seguridad de la información a la Dirección.
h) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos.
i) Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
j) Promover la mejora continua en la gestión de la seguridad de la información.

Así mismo, las diferencias de criterios que pudieran derivar en un conflicto se tratarán en el Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección General.

8.2. Roles: Funciones y responsabilidades

8.2.1. Responsable de la Información y de los Servicios

Determina los requisitos (de seguridad) de la información tratada y de los servicios prestados, según los parámetros del Anexo I del ENS. Forma parte del Comité de Seguridad de la Información y su actividad es indelegable.

Serán funciones del Responsable de la Información y de los Servicios:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.

- Dictaminar respecto a los derechos de acceso a la información y los servicios.

- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.

- La valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios y de la información será efectuada atendiendo a la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio así como el respeto a la legalidad y a los derechos de los usuarios.

- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

8.2.2. Responsable de Seguridad

Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Es independiente del Responsable del Sistema y forma parte del Comité de Seguridad de la Información siendo su actividad indelegable.

Serán funciones del Responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.

- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Aprobar la Declaración de Aplicabilidad que comprende la relación de medidas de seguridad para un sistema así como adoptar las medidas de mejora en la gestión de la seguridad de la información.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Validar y aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Constituir el punto de contacto para los aspectos relacionados con la seguridad de la información.

8.2.3. Responsable de Sistema

Es el encargado de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad.

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios e incluyendo las especificaciones, instalación y verificación del correcto funcionamiento de acuerdo a lo establecido en el Anexo II del Real Decreto 3/2010.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Notificar incidentes de seguridad de la información.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

8.3. Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por la Dirección de ASTIBOT.

Estos nombramientos se revisarán cada 4 años o cuando el puesto quede vacante.

8.4. Política de seguridad de la información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

9. Datos de carácter personal

ASTIBOT solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

10. 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 o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

11. Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de ASTIBOT en diferentes materias existentes dentro del sistema de información.

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, instrucciones técnicas, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa 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. Estará disponible para su consulta en la intranet de la organización y en su gestor documental, así como en soporte papel custodiada por la organización.

12. Obligaciones del personal

Todos los miembros de ASTIBOT 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de ASTIBOT deben estar concienciados adecuadamente en materia de seguridad TIC formándose al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de ASTIBOT, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información 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.

13. Terceras partes

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

Cuando ASTIBOT utilice servicios de terceros o ceda información a terceros, se les hará participe 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 de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información 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 el Responsable de la Información y Servicio antes de seguir adelante.

14. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

En Valladolid, a 29 de Julio de 2022

Dirección

06265985A FELIPE BETETA (R: B47736384)

Firmado digitalmente por 06265985A FELIPE BETETA (R: B47736384)
Nombre de reconocimiento (DN): 2.5.4.13=Reg:47015 / Hoja:VA-27238 /Tomo:1477 /Folio:76 /Fecha:11/03/2015 / Inscripción:1ª, serialNumber=IDCES-06265985A, givenName=FELIPE, sn=BETETA LOPEZ, cn=06265985A FELIPE BETETA (R: B47736384), 2.5.4.97=VATES-B47736384, o=ASTIBOT INGENIERIA INFORMATICA ROBOTICA Y DOMOTICA SL, c=ES
Fecha: 2022.07.29 12:55:35 +02'00'