Política de Seguridad

Autor:	*Seguridad y Organización*
Título del documento:	*Política de Seguridad*
Número de páginas	*11 (portada incluida)*
Código:	*TIR_SGR_POL*
Versión:	*01*
Fecha de última modificación:	*25 de marzo de 2024*
Clasificación:	*Pública*
	Compruebe que esta es la última versión del documento
Contactar en :	*www.tirea.es / E-mail: sau@tirea.es / Tel: 902 132 142*

Historia de Versiones

HISTÓRICO DE VERSIONES			
VERSIÓN	RESPONSABLE	FECHA	CAMBIOS INTRODUCIDOS
01	Seguridad y Organización	25/03/2024	Creación del Documento

Índice

1. Introducción

De acuerdo con la Política de los Sistemas de Gestión; "Tecnologías de la Comunicación y Redes para la Entidades Aseguradoras (TIREA) tiene como misión brindar productos y servicios de valor añadido y alta calidad al Sector Asegurador a través de aplicaciones y de una red de telecomunicaciones, que faciliten el marco normalizador de los procesos de intercambio de información que intervienen en la cadena de valor sectorial, cumpliendo con los requisitos legales y reglamentarios aplicables, y manteniendo un alto nivel de seguridad de la información y continuidad de negocio".

La Política de Seguridad de la información, a partir de aquí Política de Seguridad, tiene por objeto la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información, que constituyen los componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para los servicios de negocio de TIREA.

Por información, y activos, de la empresa se entienden desde la infraestructura informática, equipos y dispositivos de la empresa, pasando por su sistema de información interna, la propiedad intelectual e industrial, la información confidencial propia y de terceros o el know-how, hasta los diferentes tipos de datos personales que almacena y trata la empresa.

Esta Política de Seguridad es la pieza angular por la que se rigen las directrices, normas y procedimientos que debe cumplir TIREA en materia de seguridad. La presente Política de Seguridad responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en los estándares Internacionales ISO/IEC 27001 e ISO/IEC 22301, así como al cumplimiento del Esquema Nacional de Seguridad y a la legislación vigente en materia de protección de datos personales y normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a TIREA.

La Política de Seguridad deberá estar disponible en la página web corporativa de TIREA y en un repositorio común de TIREA, de forma que sea accesible por todas las personas que trabajan para TIREA.

Alcance

La Política de Seguridad es aplicable para todo TIREA, que deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible.

El alcance de la presente Política de Seguridad abarca toda la información de TIREA y de sus clientes, con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

Objetivo

El objetivo principal de la presente Política de Seguridad de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es lograr que TIREA garantice la seguridad de la información y minimice la materialización de los riesgos y el posible impacto provocado por una protección ineficaz de la información.

La Política de Seguridad es un documento aprobado por la alta dirección de la empresa, donde se compromete a garantizar la seguridad de la información y se establecen las medidas y controles que adoptará la empresa para asegurar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información, y para prevenir y mitigar los riesgos a los que se exponen los activos de información de la empresa.

2. Principios de la Política de Seguridad

Además, TIREA establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- Alcance estratégico

  La seguridad de la información cuenta con el compromiso y apoyo de los niveles directivos de TIREA para poder coordinarse e integrarse con el resto de las iniciativas estratégicas para conformar un marco de trabajo coherente y eficaz.

- Objetivos de Seguridad

  Establecer objetivos y metas específicas de seguridad. Estos objetivos dan una visión clara de lo que la empresa busca lograr en seguridad. Asimismo, permiten una medición efectiva del desempeño y el progreso hacia la mejora continua. Además, fomentan una cultura de responsabilidad y compromiso entre los empleados, reforzando así el valor que la organización otorga a la seguridad.

- Seguridad integral

  La seguridad de la información se entiende como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

- Gestión de riesgos

  El análisis y gestión de riesgos es parte esencial del proceso de seguridad de la información. La gestión de riesgos debe permitir el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles ha de realizarse mediante el despliegue de medidas de seguridad, estableciéndose un equilibrio entre los tratamientos, el impacto, la probabilidad de los riesgos a los que están expuestos, la eficacia y el coste de las medidas de seguridad.

- Proporcionalidad

  El establecimiento de medidas de protección, detección y recuperación debe ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- Mejora continua

  Las medidas de seguridad deben reevaluarse y actualizarse periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información debe ser atendida, revisada y auditada por personal cualificado. En este

ciclo de mejora continua, TIREA establece y revisa periódicamente la definición del nivel de riesgo residual aceptado (apetito al riesgo) y de sus umbrales de tolerancia.

- Seguridad por defecto

  Los sistemas se deben diseñar y configurar de modo que garanticen un grado suficiente de seguridad por defecto y mínimos privilegios. TIREA promueve que las funciones de Seguridad de la Información han de quedar integradas en todos los niveles jerárquicos de su personal y esta Política de Seguridad debe ser conocida, comprendida y asumida por todos sus empleados y colaboradores.

3. Compromiso de la Dirección

La Dirección de TIREA, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad entre todos los empleados y colaboradores.
- Exigir el cumplimiento de la Política de Seguridad, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

4. Roles y responsabilidades

TIREA se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.

TIREA nombra una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión y entre sus funciones y responsabilidades están las de aplicar principios de segregación de funciones y el contacto con las autoridades y grupos de interés especiales en materia de seguridad de la información.

La figura debe asumir las funciones que, en general, la presente Política de Seguridad atribuye a dicha figura. Su responsabilidad es desarrollar y mantener la Política de Seguridad, asegurándose que ésta sea adecuada y oportuna según evolucione tanto TIREA como la regulación vigente.

5. Cumplimiento regulatorio

TIREA se comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se ha de velar por el cumplimiento de toda legislación, normativa o regulación aplicable.

Se realizan auditorías periódicas de seguridad; el mayor beneficio de realizar una auditoría de seguridad es mejorar la cultura de una organización y establecer buenos hábitos en los empleados. Otras razones por las que las organizaciones pueden querer llevar a cabo una auditoría de seguridad son:

- Garantizar que la organización cumple la legislación, normativa o regulación aplicable; así como que gestiona los riesgos adecuadamente
- Identificar las áreas en las que la organización puede mejorar sus hábitos de seguridad
- Proponer y facilitar mejoras
- Determinar si los equipos utilizan eficazmente los programas y protocolos de seguridad

6. Gestión de la Seguridad de los Recursos Humanos

El departamento de Recursos Humanos realiza su gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad, siendo este un punto clave para asegurar su cumplimiento.

Se deben salvaguardar los requisitos establecidos en la presente Política de Seguridad en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados.

Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

TIREA debe asegurar que todo el personal recibe un nivel de formación y concienciación adecuado en materia de Seguridad de la Información en los plazos que exija la normativa vigente, especialmente en materia de confidencialidad y prevención de fugas de información. Asimismo, los empleados deben informarse de las actualizaciones de las políticas y procedimientos de seguridad afectados y de las amenazas existentes, para garantizar su cumplimiento.

7. Gestión de activos

Se debe tener identificados e inventariados los activos necesarios para la prestación de los servicios que presta TIREA. Adicionalmente, se debe mantener actualizado el inventario de activos de información.

Los empleados o colaboradores deben recibir autorización de su responsable de área para utilizar dispositivos personales en la red de TIREA.

Cada activo o elemento de información debe tener un responsable o propietario con la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido. Las configuraciones de los activos deben ser actualizadas de manera periódica, para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

TIREA gestiona adecuadamente el ciclo de vida de la información, de manera que se pueda evitar usos incorrectos durante cualquier tratamiento.

Se realizan copias de seguridad de la información, del software y del sistema y se verifican periódicamente. Para ello, se hacen copias de seguridad de aplicaciones, ficheros y bases de datos periódicamente, con las mismas medidas de seguridad que los datos originales y ubicadas en lugares seguros en un centro distinto al que las generó.

8. Clasificación de la información

Se define un modelo de clasificación de la información que permite conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad, autenticidad, trazabilidad e integridad.

La información que se considere reservada, confidencial o secreta se debe tratar con especial cuidado. Se deben definir medidas de seguridad extraordinarias o adicionales para el adecuado tratamiento de la información privilegiada. Este tipo de información se debe enviar cifrada y mediante protocolos seguros.

Se deben etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información definidos en el subapartado anterior, exceptuando la información considerada de "Uso público".

TIREA cumple con la legislación vigente sobre protección de datos personales y asegura la privacidad de estos para proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la imagen, estableciendo medidas para regular el tratamiento de los datos.

Se debe asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se debe tener en cuenta, al menos, los siguientes aspectos:

- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares
- Uso del correo electrónico
- Transmisión de información de forma oral
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Escritorios limpios y ordenados
- Equipos desatendidos.

9. Control de acceso

Todos los sistemas de información de TIREA cuenta con un sistema de control de acceso. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas y doble factor de autenticación.

El control de acceso se entiende desde la perspectiva tanto física como lógica, enfocado a sistemas de la información.

Asimismo, ningún usuario podría acceder a un sistema de información controlado sin la aprobación del responsable del sistema o de la información.

TIREA establece una norma de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La normativa de contraseñas define los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña y tiene que ser conocida por todos los empleados y colaboradores

Se controla el acceso remoto a la red de TIREA; esto es, desde fuera de las instalaciones propias. Los servicios de conexión al trabajo en remoto se destinan exclusivamente a personal de TIREA. El uso por parte de cualquier otro tipo de colaborador requerirá autorización del responsable de seguridad.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto puede ser propiedad del empleado o proporcionado por TIREA. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

a) Capacidad de realizar una conexión a través de una VPN.
b) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
c) Software antivirus instalado.
d) Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requiere de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza para la seguridad de la información de TIREA.El servicio de teletrabajo se monitoriza y controla, registrándose tanto la conexión como la actividad de acuerdo con la normativa.

10. Seguridad Física y del Entorno

Los espacios físicos donde se ubiquen los sistemas de información de TIREA están protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados a sistemas de información, robo o sabotaje) y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etc.).

11. Seguridad Operativa

Todos los sistemas de información de TIREA que procesan o almacenan información de su propiedad deben contar con las medidas de seguridad oportunas que optimicen su nivel de madurez adecuado (monitorización, control de cambios, revisiones, etc). Asimismo, se gestionan, controlan y monitorizan las redes adecuadamente, para protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que la utilizan, incluidos los controles de acceso a la red, protegiendo la información que se transfiera a través de estos elementos y/o entornos.

TIREA implanta las medidas de seguridad adecuadas para mantener la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información en la nube o cloud computing, como en cualquier otra tecnología. En el caso de la nube, estas medidas dependen de los tipos de modelo del servicio:

- Infraestructura: en primer lugar, se debe asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deben establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes están registrados y conectados para obtener la trazabilidad adecuada.
- Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio debe proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro.
- Software: de forma adicional a las medidas indicadas en el modelo de servicio de Plataforma, TIREA y el Proveedor debe seguir las buenas prácticas del mercado para la seguridad de las aplicaciones.

La arquitectura de red de TIREA cuenta con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se entiende por "dominio interno" la red local compuesta por los elementos tecnológicos de TIREA accesibles exclusivamente desde la red interna. Por otra parte, se entiende por "dominio externo" la red accesible desde el exterior de la red de TIREA.

Es de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de TIREA, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Por ello, TIREA define las pautas de seguridad de la transferencia de información, las medidas de seguridad en el uso de equipos portátiles, servicios de Internet y correo electrónico, y controles específicos para una conexión segura a los sistemas de información de TIREA desde fuera de sus instalaciones.

Toda la adquisición, desarrollo y mantenimiento de los sistemas cuenta con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, debe realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.

Cada departamento de TIREA debe tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

Se debe identificar periódicamente vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, según su exposición a dichas vulnerabilidades y adoptar medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización aplicará las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

12. Seguridad en los Proveedores

Se debe destacar la criticidad de los servicios susceptibles de subcontratar para identificar aquellos proveedores relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos a tratar o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deben cuidar los procesos de selección, requerimientos contractuales como; la terminación contractual, la monitorización de los niveles de servicio, la comunicación de incidentes, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente Política de Seguridad.

13. Gestión de Incidentes

Todos los empleados de TIREA tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, TIREA implementa procedimientos para la correcta gestión de los incidentes detectados.

La respuesta ante incidentes está procedimentada; en este procedimiento se define un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

14. Continuidad de Negocio

En respuesta a requerimientos de calidad y buenas prácticas, TIREA tiene un Plan de Continuidad de Negocio como estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe si es necesario. Este Plan de Continuidad debe ser actualizado y probado periódicamente. Además, se dispone de un Plan de Recuperación ante Desastres actualizado y alineado con la continuidad de negocio, este plan abarca la continuidad del funcionamiento de las tecnologías de información y comunicación.

TIREA se encarga de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio se revisa periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

15. Gestión de Excepciones

Cualquier excepción a esta Política de Seguridad debe registrarse e informarse al responsable de la Seguridad de la Información de TIREA. Estas excepciones se analizan para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos y su aceptación por el Comité de Seguridad, estos deben ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

16. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de TIREA. Es responsabilidad de todos los empleados de TIREA notificar al responsable de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política de Seguridad.

17. Revisión de la Política

La aprobación de esta Política de Seguridad implica que su implantación cuenta con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política de Seguridad, será revisada y aprobada anualmente por el Comité de Seguridad. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política de Seguridad permanece adaptada en todo momento a la realidad de TIREA.