POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Departamento Organización y Tecnología
Área Seguridad

ASV-POL-01
Rev nº 14

GRUPO ASV

REGISTRO DE MODIFICACIONES		
Edición	**Fecha**	**Modificación**
1	27-07-2011	Edición inicial
2	25-11-2015	Se modifican los nombres de los departamentos para ponerlos de forma más genérica
3	23-06-2016	Se amplía y modifica en su totalidad
4	15-12-2016	Revisión anual
5	15-03-2017	Aprobación Consejo de Administración
6	09-02-2018	Revisión, sin cambios y aprobación Consejo de Administración
7	21-06-2019	Revisión, actualización de normativa, cambios menores y aprobación por el Consejo de Administración
8	02-07-2020	Revisión, actualización de normativa, cambios menores y aprobación por el Consejo de Administración
9	15-02-2021	Se revisa y modifica en su totalidad
10	08-07-2021	Se incluye un nuevo apartado sobre el Criterio de Proporcionalidad. Aprobación Consejo de Administración
11	07-07-2022	Se revisa la política. Incorporación de nuevo apartado 8 sobre objetivos ODS. Aprobación Consejo de Administración
12	20-07-2023	Lenguaje Inclusivo y Nivel de Clasificación de la Información. Aprobación por el Consejo.
13	18-07-2024	Revisión con los siguientes cambios: Extracción y actualización del marco normativo a anexo 1. Aprobación por el Consejo de Administración.
14	02-12-2024	Revisión de la Política. Se incluye un nuevo apartado para el Control de las excepciones y exenciones a los controles de seguridad establecidos. Aprobación por el Consejo de Administración.

NIVEL DE CLASIFICACIÓN DE LA INFORMACIÓN: INFORMACIÓN PÚBLICA
La información relacionada con la organización clasificada como INFORMACIÓN PÚBLICA podrá circular libremente, tanto dentro como fuera de las instalaciones de la organización, sin requerir autorización expresa.

ÍNDICE

1 OBJETO

Este documento constituye la Política de Seguridad de la Información de Grupo ASV que debe ser aprobada por el Consejo de Administración. Recoge la postura de Grupo ASV en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del Grupo en cuanto a la seguridad, en la medida que ésta afecta al desempeño de sus funciones y a alcanzar sus objetivos de negocio.

2 ALCANCE

La presente Política es aplicable a todos los activos relacionados con la información de Grupo ASV, incluyendo instalaciones, sistemas de información, servicios, software y toda la información almacenada o procesada en los sistemas informáticos.

Asimismo, es de aplicación tanto a la plantilla de Grupo ASV y sus filiales como a quien provee de bienes y servicios y a cualquier persona a la que se le haya facilitado el acceso a los sistemas, instalaciones o información de Grupo ASV y sus filiales.

Todas las personas son, individual y colectivamente, responsables de entender los riesgos asociados a la información que manejan y de proteger la confidencialidad, integridad y disponibilidad de dicha información en función del valor, sensibilidad y criticidad de la misma.

3 MARCO NORMATIVO

La legislación y normativa principal cuyo cumplimiento debe observar Grupo ASV queda recogida en el anexo 1.

4 RESPONSABILIDADES

Toda la plantilla de Grupo ASV que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados por Grupo ASV que se apoyen en las TIC tienen la obligación de conocer esta Política de Seguridad y cumplirla. El Comité de Seguridad dispondrá los medios para que esta Política llegue a las personas afectadas.

5 POLÍTICA GENERAL DE SEGURIDAD

Grupo ASV utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios y es consciente de la amenaza que supone la ocurrencia de incidentes de seguridad, ya sean provocados o fortuitos, para lograr sus objetivos de negocio y para la prestación de dichos servicios. Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados, tanto desde el interior de la Organización como desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a la internet (ciber-ataques).

La política de Grupo ASV es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias y de recursos humanos. Para este fin, se establecerá una estructura de seguridad, estando formada como mínimo por un Comité

que vele por el cumplimiento de esta política, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo, de forma que se garantice:

- el cumplimiento de los objetivos de la misión de Grupo ASV y los de prestación de servicios
- el cumplimiento de la legislación y normativa aplicables

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo al negocio.
- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de aplicar medidas de seguridad, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo y, en cualquier caso, siempre que exista un riesgo de un nivel superior al máximo aceptable.

Las distintas áreas de la Organización bajo cuya responsabilidad se encuentran los servicios prestados de las líneas de negocio de Grupo ASV, deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes (dentro de sus capacidades, y/o apoyándose en el departamento experto correspondiente), las medidas de seguridad necesarias para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de la información y de los servicios.

Los requisitos de seguridad de los sistemas y servicios, las necesidades de formación de quien haga uso de ellos, quien administre y opere y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en la elaboración de requisitos utilizados para la realización de proyectos.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad:

En cuanto a la prevención, se debe evitar que la información y los servicios resulten afectados por un incidente de seguridad. Para ello, Grupo ASV implementará las medidas de seguridad que se determinen en los procesos de análisis de riesgos.

En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y respuesta a incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por personas que hagan uso de los servicios, independientemente de su procedencia (de la Organización o ajenas a esta), se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen las personas con responsabilidad en ellos, se

deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

5.1 DESARROLLO DE LA POLÍTICA

Esta Política de Seguridad se desarrollará a través de requerimientos concretos en cada uno de los procedimientos que se deriven de ésta.

Los procedimientos documentados, así como esta Política de Seguridad, se encontrarán a disposición de toda la plantilla de la organización que necesite conocerlos y, en particular, toda persona que utilice opere o administre los sistemas de información y comunicaciones, la información albergada en dichos sistemas o los servicios prestados basados en las tecnologías de la información y las comunicaciones.

5.2 FORMACIÓN Y CONCIENCIACIÓN

Toda persona con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las TIC se mantendrá correctamente formado en las tecnologías y procesos propios de su actividad y con relación con la seguridad de la información. La Dirección de Personas y Cultura gestionará los correspondientes planes y acciones formativas, pudiendo ser éstas programadas o a demanda.

Las acciones formativas deberán quedar registradas y se deberá medir su eficacia, en cuanto a aprovechamiento.

Adicionalmente, se tomarán medidas para concienciar a toda la plantilla de la organización de la importancia de mantener segura la información. Esto se realizará a través de campañas de sensibilización en materia de seguridad de la información que se llevarán a cabo periódicamente.

5.3 GESTIÓN DE RIESGOS

Los servicios bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos periódico para orientar las medidas de protección a minimizar los riesgos detectados.

Se deberá determinar el nivel de riesgo aceptable por activo para Grupo ASV. Para todos aquellos valores de riesgo que superen el umbral establecido se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo, de nuevo, a valores aceptables.

5.4 CLASIFICACIÓN Y GESTIÓN DE ACTIVOS

Grupo ASV mantendrá un inventario de los activos de información como parte importante de la administración de riesgos. Este inventario estará clasificado de acuerdo con la sensibilidad y criticidad de la información.

5.5 SEGURIDAD FÍSICA Y DEL ENTORNO

Se deberá prevenir todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información de Grupo ASV.

Se tomarán todas las medidas de seguridad razonables para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de la organización.

5.6 CONTROL DE ACCESOS

Grupo ASV impedirá el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Para ello, se implementarán procedimientos formales para controlar la identificación de quien haga uso de ellos y la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos estarán claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

5.7 COMUNICACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD

Toda persona empleada deberá informar inmediatamente, mediante el canal que se establezca al efecto, de cualquier incidente, comportamiento anómalo o situación sospechosa que pudieran detectar. Para ello se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse para solventar la situación y volver a un estado seguro. Se registrarán y definirán todos los tipos probables de incidentes relativos a seguridad asignándoles la correspondiente prioridad.

5.8 MANEJO DE DATOS PERSONALES

Para el manejo de información que incluya datos personales se observarán medidas de seguridad, técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo aceptado, tal y como exige el RGPD y la normativa española vigente asociada a la protección de datos personales Para ello se contará con la supervisión y validación del Área de Protección de Datos de GRUPO ASV.

5.9 TERCERAS PARTES

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por Grupo ASV serán hechos partícipes de esta Política (o un extracto de la misma). Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan comunicarlas.

La plantilla de las Terceras Partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, quien ejerza como Responsable de Seguridad deberá realizar un informe del riesgo en el que se incurre. Ese

riesgo deberá ser presentado al Comité de Seguridad para su aceptación, en caso de que así proceda.

5.10 CONTROL DE EXCEPCIONES Y EXENCIONES

En caso de que por alguna circunstancia se detectara la necesidad de omitir la aplicación de un control específico de seguridad, o bien autorizar el no cumplimiento de un control de seguridad debido a una circunstancia excepcional, el Responsable de Seguridad, teniendo en cuenta el control de que se trate procederá a autorizarlo o a denegarlo.

Para ello, cualquier desviación deberá estar debidamente justificada, documentada, evaluada y aprobada, atendiendo el Responsable de Seguridad a los posibles riesgos asociados. Asimismo, en función de los riesgos derivados de dichas desviaciones, se estudiarán y aplicarán medidas compensatorias que se estimen necesarias.

Todas las excepciones y exenciones se revisarán periódicamente de forma que, en el caso de que la circunstancia que derivó su aplicación haya cambiado o ya no exista, se proceda de nuevo a la aplicación del control correspondiente.

6 COMPROMISO DE LA DIRECCIÓN

La Dirección manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- Proporcionar las personas y capacidades necesarias, dentro de las posibilidades presupuestarias;
- Asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- Destinar presupuesto, dentro de las posibilidades;
- Apoyar la formación de las personas implicadas en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- Garantizar el mantenimiento de la documentación asociada a los planes;
- Promover la mejora continua.

El mencionado compromiso se manifiesta con la aprobación del presente documento.

7 CRITERIO DE PROPORCIONALIDAD

Uno de los principios esenciales en los que se asienta Solvencia II (Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio) es el de "Proporcionalidad" que, atendiendo a las obligaciones que se imponen a las entidades aseguradoras en materia de garantías financieras, reporting de información y estructura de gobierno, tiene por objeto establecer un marco jurídico equitativo para todas las entidades aseguradoras en base a la naturaleza, volumen y complejidad de las operaciones y riesgos asumidos.

En coherencia con este principio, la LOSSEAR, dispone en su artículo 65.1 que *todas las entidades aseguradoras y reaseguradoras dispondrán de un sistema eficaz de gobierno que garantice la gestión sana y prudente de la actividad y que sea proporcionado a su naturaleza, el volumen y la complejidad de sus operaciones.* Este principio se reitera en el artículo 44 del ROSSEAR.

Por ello, el artículo 110 de la LOSSEAR previene que *las actuaciones de supervisión se realizarán de forma proporcionada a la naturaleza, complejidad y envergadura de los riesgos inherentes a la actividad de las entidades aseguradoras o reaseguradoras.*

Grupo ASV, sobre la base de lo expuesto, aplicará este principio de proporcionalidad en todos sus procesos operativos y de gobierno.

8 GRUPO ASV Y LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)

Una gran mayoría de países, en el marco de la Organización de Naciones Unidas, adoptaron, en septiembre de 2015, un conjunto de objetivos globales (denominados Objetivos de Desarrollo Sostenible -ODS-) para erradicar la pobreza, proteger el planeta y asegurar la prosperidad para todos como parte de una nueva agenda de desarrollo sostenible. Cada objetivo tiene metas específicas que deberían alcanzarse en 15 años.

EL Plan Estratégico definido por GRUPO ASV impulsa su posicionamiento en diferentes ámbitos, pues no solo se ha diseñado teniendo en cuenta su impacto en la empresa y en las personas, sino, además, también en la sociedad y en el entorno natural. Bajo este prisma GRUPO ASV destaca su compromiso y asociación con los ODS, impulsados por la Organización de Naciones Unidas.

GRUPO ASV quiere aportar valor a la sociedad y por eso se enfocará principalmente en los siguientes objetivos de la agenda 2030: Salud y Bienestar, Igualdad de Género, Trabajo Decente, y Crecimiento Económico, Consumo Responsable y Acción por el Clima.

9 REVISIÓN Y MODIFICACIÓN DE LA POLÍTICA

La política de seguridad de la información será revisada al menos, anualmente, o cuando ocurran cambios significativos para asegurar la continua idoneidad, eficacia y efectividad de la misma. Cualquier cambio requerirá del acuerdo y aprobación por parte del CA.

10 ANEXO 1: MARCO NORMATIVO APLICABLE

Este anexo pretende recopilar las principales normativas aplicables a nivel global y por línea de negocio.

10.1 Marco normativo global

Norma	Descripción breve
Reglamento (UE) 2016/679	Reglamento General de Protección de Datos (RGPD)
Ley Orgánica 3/2018 LOPDGDD	Protección de Datos Personales y garantía de los derechos digitales
Real Decreto Legislativo 1/1996	Texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes en la materia.
Real Decreto Legislativo 2/2015	Texto refundido de la Ley del Estatuto de los Trabajadores.
Instrucción 1/1996	Ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios
Instrucción 1/2006	Tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
Ley 34/2002	Servicios de la sociedad de la información y de comercio electrónico.

10.2 Marco normativo Transporte Sanitario

Norma	Descripción breve
RD 311/2022 ENS	Regulación del Esquema Nacional de Seguridad
ISO 27001 (voluntario)	Sistemas de Gestión de la Seguridad de la Información (SGSI)
ISO 27002 (voluntario)	Controles para el tratamiento de riesgos en un SGSI
Resolución de 7 de octubre de 2016, de la SEAP	Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad
Resolución de 27 de marzo de 2018, de la SEAP	Aprobación de la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información
Resolución de 13 de abril de 2018, de la SEAP	Aprobación de la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
Ley 14/1986	Ley General de Sanidad
Ley 33/2011	Ley General del Salud Pública
Ley 41/2002	Básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
Ley 10/2014	Salud de la Comunidad Valenciana
Real Decreto 836/2012	Características técnicas, equipamiento sanitario y dotación de personal en vehículos de transporte sanitario por carretera.
Decreto 157/2014	Establecimiento de autorizaciones sanitarias y gestión de registros de ordenación santiaria de la Conselleria de Sanitat.

10.3 Marco normativo Seguros

Norma	Descripción breve
Directiva 2009/138/CE	Función de verificación de cumplimiento
Reglamento (UE) 2022/2554	Resiliencia Operativa Digital del sector financiero
Directiva (UE) 2022/2556	Resiliencia Operativa Digital del sector financiero
Reglamento Delegado (UE) 2015/35	Acceso a la actividad de seguro y de reaseguro
Ley 30/1995	Ordenación y Supervisión de los Seguros Privados
Ley 50/1980	Regulación del Contrato de Seguro
Real Decreto Legislativo 6/2004	Texto refundido de la Ley de ordenación y supervisión de los seguros privados
Ley 20/2015	Ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras
Real Decreto 2486/1998	Reglamento de Ordenación y Supervisión de los Seguros Privados
Real Decreto 1060/2015	Ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras
REGLAMENTO DE EJECUCIÓN (UE) 2017/1469	Formato de presentación normalizado para el documento de información sobre productos de seguro
Real Decreto Legislativo 1/2007	Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
Ley 3/2014	Modificación RDL 1/2007
Regulación general sector seguros	

10.4 Marco normativo Servicios Funerarios

Norma	Descripción breve
RD 311/2022 ENS	Regulación del Esquema Nacional de Seguridad
Resolución de 27 de marzo de 2018, de la SEAP	Aprobación de la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información
Resolución de 13 de abril de 2018, de la SEAP	Aprobación de la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
Ley 20/2011	Ordenación jurídica del Registro Civil
Decreto 2263/1974	Aprobación del Reglamento de Policía Sanitaria Mortuoria
Decreto 39/2005	Regulación de prácticas de policía sanitaria mortuoria en Comunidad Valenciana
Decreto de 14 de noviembre de 1958	Aprobación del Reglamento para aplicación de la Ley del Registro Civil
Decreto 95/2001	Reglamento de Policía Mortuoria (Andalucía)
Decreto 129/2023	Sanidad Mortuoria (Galicia)
Decreto 132/2014	Sanidad Mortuoria (Canarias)
Reglamento de sanidad mortuoria de la ciudad de Ceuta	