SYNECTIC

ABSoftware

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD

ISO 22301 Continuidad de Negocio
ISO 27001 Seguridad de la Información
ENS – Esquema Nacional de Seguridad
ENSI-C4V Esquema Nacional de Seguridad Industrial
Leet Security Rating System

Agbar

Datos del documento	
Título	Política del Sistema de Gestión de Seguridad
Tratamiento	Pública

Control de versiones			
Versión	Descripción	Fecha	Autor
1.0	Adaptación de la política previa	18/10/2017	OCN
1.1	Referencias a Políticas de rango superior	26/10/2018	OCN
1.2	Alineación con normas transversales	08/03/2019	KGV
1.3	Revisión	20/4/2020	RCN
1.4	Alineación SGSI ABS y Synectic a esta política	02/02/2022	IT Governance

Índice

1 Objetivo

Esta política, recoge y describe de forma general las actividades y procesos (acciones, reglas y regulaciones) de carácter obligatorio diseñadas para soportar la estructura de la normativa de seguridad que a su vez soportan los objetivos recogidos en la Política de Seguridad de la Información y uso de las Tecnologías de la Información y Comunicación (en adelante "**Política de Seguridad TIC**") de **Agbar.**

Con la finalidad de garantizar la **integridad**, **disponibilidad** y **confidencialidad**, así como la trazabilidad de la información que es tratada por la organización.

2 Alcance

El presente documento, es de obligado cumplimiento en el ámbito de AGBAR, para todos los usuarios de Aqualogy Business Software y Synectic Tecnologías de la Información (en adelante LAS ORGANIZACIONES o LAS COMPAÑÍAS) que desarrollan sus actividades dentro del alcance definido del Sistema de Gestión de Seguridad.

Del mismo modo, este procedimiento general es complementario y no excluyente con las Políticas de rango superior existentes en la compañía:

- Política de Seguridad de la Información y uso de las TIC

3 Definición

- **Política de seguridad**

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

- **Principios básicos de seguridad**

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

- **Sistema de gestión de la seguridad (SGSI)**

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

de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- **Sistema de información**

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

- **Información**

Caso concreto de un cierto tipo de información.

- **Responsable de la información**

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

- **Responsable de la seguridad**

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- **Responsable del servicio**

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

- **Responsable del sistema**

Persona que se encarga de la explotación del sistema de información.

- **Responsable del SGSI**

Persona dentro de la organización de LAS COMPAÑÍAS que se encarga de la gestión del SGSI según se define en los roles y puesto de trabajo.

- **Servicio**

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

- **Análisis de riesgos**

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

- **Datos de carácter personal**

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Personales y garantía de los Derechos Digitales.

- **Equipos móviles**

Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

- **Gestión de incidentes**

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

- **Gestión de riesgos**

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

- **Incidente de seguridad**

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

- **Trazabilidad**

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

- **Vulnerabilidad**

Una debilidad que puede ser aprovechada por una amenaza

4 Desarrollo

4.1 Aspectos Generales

La evolución y auge de las nuevas tecnologías de la información y la comunicación (TIC) está generando en nuestra sociedad un cambio sustancial en las relaciones personales entre individuos, pero también en el mundo empresarial y de los negocios. La ciberseguridad está recobrando una importancia vital.

Las sociedades y los servicios que las sustentan se enfrentan a nuevas amenazas, riesgos transversales, interconectados y transnacionales como son: los desastres naturales, el terrorismo internacional y la cibercriminalidad.

Estos servicios son prestados gracias a grandes infraestructuras que han sido desarrolladas y perfeccionadas durante los últimos años por compañías de los diferentes sectores.

Los retos de seguridad más relevantes del ciberespacio tienen que ver con los incidentes que impactan directamente en la confianza digital de los ciudadanos y empresas, pero también en el propio bienestar de las personas, la ciberdefensa y la seguridad y protección de las infraestructuras.

Es necesario proveerse de soluciones técnicas, aplicar adecuadas medidas de seguridad, y aumentar nuestra capacidad de detección y respuesta, planificando nuestras actuaciones en situaciones altamente adversas.

Asimismo, estamos en un entorno altamente regulado, y por tanto, directa o indirectamente estamos obligados al cumplimiento de:

- 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) y su Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos
- Por su parte la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos consagra el derecho de los ciudadanos a comunicarse electrónicamente con las Administraciones Públicas, lo que implica la necesidad de, como prestación de servicios de a compañías públicas y público privada, debemos adoptar medidas que garanticen una adecuada protección de los sistemas, los datos, las comunicaciones y los servicios electrónicos. El Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero, pretende dar respuesta a esta necesidad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Personales y garantía de los Derechos Digitales.
- Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información en la que se establecen mecanismos que, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información.
- Otra legislación aplicable, en registro detallado a tal efecto (véase PS18-Cumplimiento).

- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto 951/2015, de 23 de octubre, de modificación del 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.

4.2 La Política del Sistema de Gestión de Seguridad

El Comité del Sistema de Gestión de Seguridad, consciente de la importancia que la dirección de AGBAR tiene de la Seguridad en todos los ámbitos de la organización, define esta Política alineada con la Política TIC de Agbar, proporcionando un marco para el establecimiento de objetivos, basándose en los siguientes compromisos:

- **Contribuir desde la gestión de la seguridad al cumplimiento de la misión y objetivos de AGBAR.**
- **Inversión constante y responsabilidad de la seguridad** estableciendo los medios necesarios y adecuados para proteger y garantizar la seguridad de personas, procesos, información y sistemas.
- **Extender el compromiso con la seguridad a** terceros, empleados y directivos del Grupo, los cuales deberán conocer y respetar las medidas adoptadas por la compañía.
- **Desarrollo y adaptación continua**. La presente política se especifica y desarrolla a través de normas, guías, estándares, circulares, manuales y procedimientos, que se irán actualizando cuando sea necesario en función de las nuevas exigencias (estratégicas, tecnológicas, legales o reglamentarias, etc.).
- **Fomento de una cultura empresarial resiliente y consciente de la Seguridad basada en concienciación y formación del personal** a empleados/as y a colaboradores, previniendo la aparición de incidentes de seguridad por comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible.
- **Garantizando el cumplimiento legal y/o regulatorio,** de nuestros grupos de relación, relativos a la seguridad de la información y/o de los servicios.
- **Integrando la gestión de riesgos** como parte del proceso de toma de decisiones y consecución de objetivos minimizando al máximo el riesgo con esfuerzos razonables.
- **Implantando medidas de seguridad legales, técnicas y organizativas** adecuadas, proporcionadas y razonables (conforme al valor y criticidad de los activos), preventivas, de detección y correctivas frente a posibles conductas delictivas y a aquellos riesgos que

puedan influir en la correcta ejecución de servicios o en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

- **Asegurar la continuidad del negocio,** estableciendo las medidas necesarias para poder responder de forma adecuada ante un incidente disruptivo y reducir su impacto.
- Establecer como **marco para la gestión de la seguridad y compromiso de mejora continua** las siguientes normas de referencia:
    - ISO 27001 Seguridad de la Información
    - ENS – Esquema Nacional de Seguridad

Estos compromisos servirán de base tanto para el establecimiento de objetivos como la determinación de estrategias/objetivos del propio Sistema de Gestión de Seguridad.

Existen otras normas, directrices y modelos adoptados por la organización que han sido valorados en el contexto general, y que de la misma manera deberán ser tenidos en cuenta.

Con respecto a la gestión de riesgos, la organización ha definido una metodología de apreciación de riesgos propia en función al marco establecido para la gestión de la seguridad utilizando como referencias las normas ISO 22301, ISO 27001, ENS, ENSI – C4V y LSR (véase F03_01 Metodología análisis de riesgos).

4.3 Revisión de la política

Con relación a las revisiones que puedan realizarse sobre la redacción del texto que constituye la política del Sistema de Gestión de Seguridad, se realizarán revisiones y oportunos cambios, **anualmente**, y/o siempre que se produzcan cambios o eventos significativos de seguridad.

4.4 Organización de la seguridad

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen los objetivos propuestos en la presente política requieren del establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad.

Para ello, se ha establecido un **Comité del Sistema de Gestión de Seguridad**, con las funciones requeridas por los sistemas de gestión implantados (ISO 27001) y alineadas con los requerimientos de Seguridad como función diferenciada (Art. 10 ENS -> Responsable de Seguridad, Responsable del Servicio y Responsable de Seguridad de la Información).

Las funciones están documentadas en el registro correspondiente (véase PS06 - Organización de la seguridad de la información).

Del mismo modo, debe tenerse en consideración que AGBAR cuenta con una organización de la seguridad (complementaria y no excluyente de este sistema de gestión) específica en materia

de Protección de Infraestructuras que, por su carácter reservado, se encuentra separada de la citada documentación.

En el caso de presentarse conflictos en las atribuciones de cada responsable, será el Director de Seguridad Corporativa quien interceda y determine las funciones y responsabilidades.

4.5 Autoridad sobre la Política

Corresponde al Comité del Sistema de Gestión de Seguridad la autoridad para verificar el cumplimiento de su Política, y la responsabilidad de hacer cumplir las directrices generales, con independencia para plantear cuántas acciones sean necesarias para desarrollar el sistema de Gestión, así como el ENS cumpliendo los objetivos y garantizando la mejora continua.

4.6 Comunicación de esta Política

La presente Política será objeto de comunicación a la totalidad de usuarios [1] que se encuentran implicados en el alcance del Sistema de Gestión de Seguridad, mediante cauces habituales de notificación.

4.7 Obligaciones del personal

Todo el personal con responsabilidad en el **uso, operación, y/o administración** de los sistemas implicados en el alcance del Sistema de Gestión de Seguridad implantado, tienen la **obligación de conocer y cumplir esta Política**, así como los procedimientos (generales y/o de seguridad) con independencia del tipo de relación jurídica que les vincule con AGBAR.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité del Sistema de Gestión de Seguridad, con el apoyo del departamento de recursos humanos, promoverá un programa de concienciación.

El **incumplimiento de esta Política**, y/o de los procedimientos de desarrollo de este sistema de gestión (generales y de seguridad), así como las normas y procedimientos transversales de seguridad de AGBAR, dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

4.8 Entrada en vigor

[1] A efectos del Sistema de Gestión de Seguridad, hace referencia tanto a empleados de LAS COMPAÑÍAS como al personal subcontratado o de empresas colaboradoras, con independencia de su ubicación siempre que se encuentren involucrados en las actividades bajo el alcance de certificación

La presente Política entrará en vigor al día siguiente de su aprobación.

5 Referencias Normativas

Normas externas

- ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información (SGSI).
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.
- 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.
- ENS Esquema Nacional de Seguridad. [ORG.1] Política de Seguridad.
- Así como las restantes normas jurídicas que inciden parcialmente en la materia objeto de este procedimiento, contenidas en el denominado Código de Derecho de la Ciberseguridad, publicado en el BOE en formato electrónico, de acuerdo con su última actualización.

Normas internas

- Política de Agbar de Seguridad de la Información y uso las TIC.
- Política de Uso de Herramientas informáticas.
- Política de Privacidad – Directrices para empleados.
- Buenas prácticas en el tratamiento de datos personales RRHH.
- Política de conservación de datos y almacenamiento en soporte papel

- Política de Gestión de brechas de Seguridad
- Política de Protección de datos desde el diseño y por defecto en el desarrollo de aplicaciones.

6 Disposiciones Derogatorias

La Política y los procedimientos conexos derogan cualquier otro que le contradiga, dentro de los límites del alcance del Sistema de Gestión de Seguridad implantado.

7 Registros

No se define.

8 Anexos

No se define.

Firma: Luís Alfonso Navarrete López

CIO en Agbar

Director de Sistemas de Información • Dirección Estrategia IT

Firmado por :
50969109M LUIS ALFONSO NAVARRETE (R: A61821526)
DIRECTOR GENERAL
DIRECCIÓN GENERAL
SYNECTIC, TECNOLOGÍAS DE LA INFORMACIÓN, S.A.U.
2022-05-11 07:15:48 UTC