VALORIZA

POLÍTICA DE SEGURIDAD DE LA INFORMACION

v.1.0

INDICE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de VALORIZA SERVICIOS MEDIOAMBIENTALES, S.A., en adelante, "VALORIZA", en el marco de su competencia de establecer las políticas y estrategias generales de la Sociedad, ha aprobado la presente Política de Seguridad de la Información (en adelante, la "Política").

El objetivo de esta Política, dirigida a todos los grupos de interés, es el de definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información.

1 Finalidad.

VALORIZA y su grupo de sociedades, asumen la seguridad de la información asociada a sus servicios como uno de los factores clave en la realización de sus actividades con el objeto de garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, protegiendo los datos y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.

Forma parte de la política estratégica de VALORIZA la implantación y desarrollo de un Sistema de Gestión de Seguridad de la Información basado en la identificación, protección, detección, respuesta y recuperación de los sistemas de información, aportando para ello la Alta Dirección, los recursos necesarios para su consecución.

VALORIZA entiende que los procesos asociados a la seguridad de la información no pueden imponerse desde fuera, sino que deben nacer desde el interior del equipo humano que forma la Sociedad, y anima a todas las personas de la misma a hacer de la seguridad de la información su forma de trabajo. A tal efecto, la Dirección de VALORIZA se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información implantado, en las revisiones periódicas que mantiene cada año y mediante el establecimiento de objetivos y acciones de mejora.

2 Ámbito de aplicación

La presente Política es de aplicación a todas las sociedades filiales o participadas mayoritariamente respecto de las que, de forma directa o indirecta, se ejerza un control efectivo por parte de VALORIZA independientemente de su localización geográfica. Por lo tanto, en todas las referencias que esta Política haga a VALORIZA, se entenderán incluidas todas las sociedades detalladas anteriormente.

No están incluidas en su ámbito de aplicación las sociedades filiales o participadas minoritariamente respecto de las que no se ejerza, ni de forma directa ni indirecta, un control efectivo por parte de VALORIZA, que dispondrán, en su caso, de sus propias políticas o normativa interna que regule la materia, no pudiendo en ningún caso, éstas ser contrarias a lo establecido en la presente Política.

3 Principios Generales

Mediante esta Política, VALORIZA y las demás sociedades del Grupo asumen y promueven los siguientes principios generales que deben guiar todas sus actividades:

a) Dirigir nuestros esfuerzos a la prevención de errores, así como a su corrección y control
b) Fomentar la participación de todos para conseguir los objetivos establecidos por la empresa lo que redundará en el bien de nuestros clientes y otros grupos de interés
c) Impulsar la formación continua y la concienciación en materia de seguridad de la información
d) Asegurar que la empresa cumple con los requisitos de los clientes, además de con los requisitos legales y reglamentarios aplicables, haciendo especial foco en aquellos establecidos por la legislación en materia de seguridad de la información
e) Establecer acciones sistemáticas de control, monitorización y prevención de incidentes de seguridad
f) Dotarse de herramientas y procedimientos que permitan adaptarse con agilidad a las condiciones cambiantes del entorno
g) Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, protegiendo los datos y los sistemas de información contra los accesos indebidos, ciberataques y modificaciones no autorizadas
h) Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos
i) Realizar una adecuada evaluación, gestión y tratamiento del riesgo de seguridad de la información para alcanzar un nivel de madurez elevado y minimizar el riesgo, priorizando las medidas y controles a implantar acordes con los riesgos identificados y objetivos de negocio
j) Actuar de manera adecuada y conjunta para prevenir, detectar y responder a los ciberincidentes que pudieran afectar a la seguridad de la información
k) Mejora de la eficiencia de los controles de seguridad implantados para adaptarse a la evolución de los riesgos y los nuevos entornos tecnológicos
l) Revisar y evaluar la seguridad de la información periódicamente tomando las medidas necesarias para corregir las desviaciones que se pudieran presentar

Esta política de seguridad de la información ha sido aprobada por el Consejero Delegado el 23 de noviembre 2023