POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.INTRODUCCIÓN

La Política de Seguridad de la Información (en adelante, Política) persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres 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 en FONTANERÍA VISTA ALEGRE S.L. (FONTAVIS).

A continuación, se describen los principios donde se sostiene la Política de Seguridad de la Información de nuestra organización. Este conjunto de principios fundamentales ha sido formulado basándose en necesidades válidas de negocio, reconocimiento del valor añadido de los sistemas a proteger y una compresión de los riesgos asociados a estos sistemas.

2.OBJETO

El propósito de esta Política de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información.

3.ALCANCE

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI) y a todos los empleados de FONTAVIS, así como las partes interesadas que realicen tratamientos de información propiedad de FONTAVIS.

4. APROBRACIÓN Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA

Dirección es el responsable de la aprobación de la Política de Seguridad de la Información, siendo el Responsable de Seguridad quien la elabora y revisa. Cualquier cambio o evolución que afecte o pudiera afectar al contenido de la Política de Seguridad de la Información quedará registrado en una nueva firma del documento de aprobación.

La Política de Seguridad de la Información debe ser difundida a todas las partes interesadas para su fiel cumplimiento.

Con frecuencia anual, en caso de no requerir modificaciones, será revisada con la finalidad de verificar su idoneidad.

5.PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de FONTANERÍA VISTA ALEGRE S.L. (FONTAVIS), entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de los servicios de la organización, y, por tanto, soporta los siguientes objetivos y principios:

La Seguridad de la Información deberá contar con el compromiso y apoyo de todos los niveles de la organización para conformar un marco de trabajo completamente coherente y eficaz.

La Seguridad de la Información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, así como deberá considerarse como parte de la operativa habitual.

El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

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.

Se asegurará el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

La Dirección deberá asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

Se establece el compromiso de mejorar continuamente la seguridad mediante el establecimiento y seguimiento periódico de objetivos de seguridad de la información.

6.CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

FONTAVIS definirá un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en el presente apartado de la Política.

Se clasifica la información en función del soporte en el que está siendo utilizado:
a) Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.
b) Soportes físicos: información que esté en papel, soportes magnéticos, etc.

De igual forma, debe clasificarse la información en función de su uso:

- Uso público
- Difusión limitada
- Información confidencial
- Información reservada
- Información secreta

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada.

Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.

La información privilegiada estará en todo momento custodiada durante todo el ciclo de vida de la misma.

Los dispositivos móviles empleados son controlados solicitando autorización para su salida.

Cada dispositivo dispone de acceso personalizado siendo custodiado por el Responsable de Seguridad.

7.CONTROL DE ACCESO

FONTAVIS dispone de un sistema de control de acceso a los sistemas de información. El control de acceso debe asegurar el acceso de los usuarios y prevenir el acceso no autorizado incluyendo medidas como la protección mediante contraseñas. El control de acceso se entenderá desde la perspectiva tanto lógica como física.

Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.

8. SEGURIDAD FÍSICA Y EN EL ENTORNO

Los espacios físicos donde se ubiquen los sistemas de información de **FONTAVIS** deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia 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.).

9. SEGURIDAD EN LA OPERATIVA

FONTAVIS implementa medidas para gestionar, controlar y monitorizar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluidos los controles de acceso a la red, protegiendo así toda la información que se transfiera a través de estos elementos y/o entornos.

10. SEGURIDAD CON PROVEEDORES

Los proveedores se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, 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.

Es de obligado cumplimiento para todos nuestros suministradores las directrices establecidas que se indican a continuación:

•Cumplir con la política de seguridad de la información
•Mantener un cifrado adecuado en todas las comunicaciones entre su parte y FONTAVIS.

•Si se necesita acceso a la organización, la persona invitada deberá acreditarse en la entrada del edificio e ir acompañada en todo momento por un empleado de FONTAVIS

Esta regulación en materia de seguridad incide en los siguientes campos de la organización:
Acceso a las instalaciones.
En la que se regulan las normas de acceso, haciendo especial mención a los accesos a áreas seguras y regulación del acceso a personas ajenas a la organización.
Acceso a la red corporativa.
Los recursos corporativos son protegidos con los medios de seguridad técnicos necesarios para asegurar la protección de la información, ya sea desde las propias instalaciones o de forma externa. El acceso y el uso de la información están reguladas por normas enfocadas a la protección con especial atención a información sensible o confidencial.
Uso de los activos.
Las personas en FONTAVIS se comprometen a hacer un uso racional y velar por el cuidado de los equipos proporcionados por la organización para el desempeño de sus funciones y tareas. En este sentido se describen normas de actuación y se aplican configuraciones encaminadas a la protección de la información contenida en estos dispositivos.
Uso de Internet.
Especial atención se realiza en la regulación del uso de Internet, correo electrónico y almacenamiento en la nube a usos profesionales con el objetivo de minimizar riesgos que puedan producirse con un uso no regulado de dichas herramientas.
Gestión de incidencias.
La implicación de las personas de FONTAVIS en materia de seguridad ayuda a detectar posibles problemas que puedan poner en peligro la confidencialidad, integridad y disponibilidad de los servicios o activos que soportan.

Continuidad de negocio
Todos los medios implantados para la disponibilidad y continuidad del negocio en línea con los requerimientos de los esquemas ISO certificados en la organización.

Propiedad intelectual.
Protegida con el compromiso de las personas de FONTAVIS conforme a las normas de confidencialidad de la Organización.

El no cumplimiento de las pautas establecidas, está sujeta a sanción de acuerdo con los mecanismos habilitados en la legislación vigente y a la normativa interna de la corporación.

11. RECURSOS HUMANOS

FONTAVIS deberá 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.

PUESTO DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA

Existe política de puesto despejado y bloqueo de pantalla definida en la Política de Seguridad de la Información de **FONTAVIS.**
No se almacena información en los escritorios, todo se almacena dentro del NAS Server, en el directorio especificado para cada tipo de documentación.

En el escritorio, todos los documentos impresos o soportes de almacenamiento de datos que contengan información sensible, y con los que no se esté trabajando en ese momento, deben ser archivados o retirados de la mesa o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar que sean visibles o accesibles por personal no autorizado. Deberá guardarse la

máxima discreción con los documentos en uso, a fin de evitar accesos accidentales por personal que visite nuestro puesto.

Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo con lo establecido en el documento de Política de clasificación, etiquetado y manejo de la información.

Las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deben estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuanto el responsable de un puesto de trabajo lo deje sin atención, bien temporalmente o bienal finalizar su trabajo, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto se puede realizar a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo tiene que implicar la desactivación de la pantalla protectora con la autenticación del usuario. En lo que respecta a la documentación, esta no deberá dejarse expuesta.

En el caso de las impresoras debe asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos.
Los puestos de trabajo tienen una configuración fija en sus aplicaciones y sistemas operativos, que sólo puede ser cambiada por las personas autorizadas para ello. Este punto es extensible a la instalación o actualización de aplicaciones.
Los ficheros temporales que el personal mantenga en su equipo deberán ser borrados, una vez haya concluido la finalidad para la que fueron creados (fichero temporal: ficheros de trabajo creados por los usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento).
Se prohíbe la realización de nuevos tratamientos de datos personales sin previa autorización de la organización.
Se prohíbe ceder datos personales sin autorización.
Se prohíbe utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales.
Los puestos asignados a cada persona se consideran herramientas de trabajo, y pueden ser revisados y accedidos desde dirección en el caso de ser necesario. El acceso al puesto de trabajo no requerirá preaviso previo.

12. CIFRADO

FONTAVIS emplea controles y claves criptográficas para la protección de la integridad, confidencialidad, trazabilidad y autenticidad de la información siempre que lo especifiquen la legislación o la normativa interna de seguridad de la información.

Toda la información clasificada como confidencial, lo que incluye a los datos de carácter personal de nivel alto, deberá ser encriptada para su transmisión, transferencia o salida de las oficinas de **FONTAVIS** en cualquier soporte que se considere adecuado según se identifica por Responsable de Seguridad.

Se utilizarán controles y claves criptográficas para la protección de la integridad, confidencialidad, trazabilidad y autenticidad de la información siempre que lo especifiquen la legislación o la normativa interna de seguridad de la información.

Toda la información clasificada como confidencial, lo que incluye a los datos de carácter personal de nivel alto, deberá ser encriptada para su transmisión, transferencia o salida de las oficinas de **FONTAVIS** en cualquier soporte que se considere adecuado según se identifica por Responsable de Seguridad.

La simple ofuscación de la información no es un método de encriptación y por lo tanto no puede utilizarse como medida de protección de la información en general y de forma particular de la confidencial.

Las claves de encriptación y los certificados digitales se consideran a los efectos de la clasificación de la información como información confidencial.

Las claves y certificados utilizados en los controles criptográficos deben almacenarse de forma segura en repositorios protegidos siguiendo las indicaciones definidas y con acceso estrictamente limitado a los usuarios autorizados, que han tenido que ser autorizados previamente por el responsable de Seguridad. En particular, se procurará no guardar claves en equipos portátiles o en documentos físicos.

El compromiso o sospecha de compromiso de los elementos utilizados en los controles criptográficos debe ser tratado como una incidencia de seguridad grave. Los elementos comprometidos deberán ser revocados y reemplazados a la mayor brevedad.

Se exceptuará los certificados de los servidores web internos ya que estos no están accesibles desde el exterior y se encuentran en entornos controlados. Así mismo, se podría añadir excepciones puntuales que fueran aprobadas previamente por el responsable de seguridad.

13. INTERCAMBIO DE INFORMACIÓN

Cuando se realicen acuerdos entre organizaciones para el intercambio de información digital y software, se especificará el grado de sensibilidad de la información del organismo involucrado y las consideraciones de seguridad sobre la misma.

INTERCAMBIO DE INFORMACIÓN CONFIDENCIAL

El correo electrónico no puede ser empleado para la transmisión de datos confidenciales de manera no justificada ni para fines diferentes a los establecidos para el correcto desarrollo de sus funciones laborales.

Se prohíbe la comunicación de información confidencial fuera de la organización salvo aprobación expresa por parte del responsable de esta.

Todo el personal o terceros que accedan a la información de la organización tendrán que aceptar un acuerdo de confidencialidad y no revelación de la información de la que hayan sido conocedores.

USO DE LAS CUENTAS DE CORREO Y MENSAJERÍA DE LA ORGANIZACIÓN

Las cuentas de mensajería o correo electrónico de la organización nunca se considerarán personales o privadas.
Se prohíbe la utilización de las herramientas de mensajería y del correo electrónico corporativo para usos personales o particulares. Se consideran herramientas de trabajo, y como tal podrán ser revisadas en caso de incidencia, y desviado en caso de ausencia o baja del trabajador, sin necesidad de previo aviso.
Usos de cuentas de mensajería o correo electrónico externas

No se autoriza el uso de cuentas de correo electrónico fuera del dominio de la organización, salvo autorización de algún miembro del comité de seguridad por motivos razonados, y quien se encargará de tener posibilidad de acceso a las mismas.

14. SANCIONES

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias por parte de **FONTAVIS**.

Es responsabilidad de todos los empleados 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.

Cartagena, 05 de Abril de 2023 Rev 1

José Antonio López Lorca

FONTAVIS
FONTANERÍA VISTA ALEGRE, S.L.
C.I.F. B30901474
Fontanería, Gas, Calefacción, ACS y Energía Solar
C/ Mayor, nº 17 - Vista Alegre - 30399 Cartagena

Gerente