

Título:	Política de Seguridad de la Información	
Código:	GF_PYCS002	
Revisión nº:	1	
Aplicable a :	Protección y Ciberseguridad	
Responsable emisión:	Coordinador General de Protección y Ciberseguridad Delegada de Protección de Datos	
Revisado por:	Director Industrial Grupo Fertiberia	Fecha: 18 de junio de 2021
		Firma:
Aprobado por:	Consejero Delegado Grupo Fertiberia	Fecha: 18 de junio de 2021
		Firma:

Resumen modificación: Rev. 1: Documento inicial

Lista inicial de distribución:

- Comité de Dirección Grupo Fertiberia
- Comité de Dirección ADP
- Direcciones Generales Empresas del Grupo Fertiberia
- Direcciones Corporativas del Grupo Fertiberia
- Direcciones de Fábrica y Centros de Trabajo Grupo Fertiberia
- Coordinador General de Protección y Ciberseguridad
- Coordinadores Generales QHSE Grupo Fertiberia
- Coordinadores de Seguridad Fábricas y Centros Grupo Fertiberia

Índice

1. Introducción
2. Ámbito de aplicación
3. Alcance
4. Compromiso con la Dirección
5. Política de Seguridad
 - 5.1 Gestión y evaluación del riesgo
 - 5.2 Políticas y Requisitos de Conformidad de la Seguridad
 - 5.2.1 Aspectos organizativos de la seguridad de la información
 - 5.2.2 Seguridad relativa a los RRHH
 - 5.2.3 Gestión de activos
 - 5.2.4 Control de accesos
 - 5.2.5 Seguridad física y del entorno
 - 5.2.6 Seguridad de las operaciones
 - 5.2.7 Seguridad de las comunicaciones
 - 5.2.8 Adquisición, desarrollo y mantenimiento de los Sistemas de Información
 - 5.2.9 Relación con Proveedores
 - 5.2.10 Gestión de incidentes de seguridad
 - 5.2.11 Aspectos de seguridad de la información para la gestión de la continuidad de negocio
 - 5.2.12 Cumplimiento

1. Introducción

La Información, es uno de los activos más importantes para una organización y, por lo tanto, debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se transmita, almacene o procese.

Grupo Fertiberia, consciente de la importancia del valor de su información dispone de marco normativo en materia de seguridad de la información, apoyado en un proceso de mejora continua cuya finalidad es gestionar la seguridad, garantizar la integridad y disponibilidad de la información almacenada, transmitida o procesada por los Sistemas de Información y comunicaciones de los cuales son responsables.

La Política de Seguridad relativa a los Sistemas de la Información, establece una serie de objetivos orientados a proteger su información y los sistemas que la soportan frente a posibles amenazas, reducir los daños provocados por incidentes y asegurar la continuidad de sus servicios, preservando los criterios básicos de seguridad:

- Confidencialidad: Garantizar que a la información y a los sistemas sólo acceden las personas debidamente autorizadas.
- Integridad: Garantizar la exactitud de la información y los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Disponibilidad: Garantizar que la información y los sistemas puedan ser utilizados en la forma y tiempo requeridos.

Los parámetros anteriormente descritos, son esenciales para el cumplimiento de la legislación vigente en materia de seguridad de la información y para la prestación de un servicio de calidad.

2. Ámbito de aplicación

Esta Política de Seguridad, afecta a los Sistemas de Información, siendo aplicable con carácter obligatorio a todo el personal del Grupo Fertiberia, en el entendido que comprende tanto Fertiberia como todas las entidades de su grupo empresarial. De la misma forma se aplica a las entidades colaboradoras que hagan uso de la información y de los sistemas que la soportan propiedad de esta.

La Política de Seguridad de Fertiberia, toma como referencia los criterios de las normas UNE ISO/IEC 27001:2017, UNE ISO/IEC 27002:2017, ISO/IEC 27017:2015, ISO/IEC 27018:2019 y UNE ISO/IEC 22301:2015, de manera que adopta las precauciones necesarias para garantizar el nivel de seguridad

exigido por el marco legal vigente en materia de seguridad de la información, especialmente la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, las normas que la transponen y desarrollan en los ámbitos del Derecho español, francés y portugués y; el Reglamento UE 2016/679 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 -en adelante, Reglamento de Protección de Datos o RGPD- y las normas que lo complementan en el ámbito del Derecho español, francés y portugués.

3. Alcance

El alcance de la Política de Seguridad, son todos los Sistemas de Información del Grupo Fertiberia, así como todo el personal implicado o que haga uso de estos.

4. Compromiso con la Dirección

El Comité de Seguridad es consciente de la importancia que tiene para Grupo Fertiberia la seguridad de la información. Por esta razón, ha desarrollado la presente Política de Seguridad, y quiere dejar constancia de su apoyo, aprobación y asignación de los recursos necesarios para su ejecución y está distribuida a todo el personal para que la conozca y cumpla.

5. Política de Seguridad de la Información

5.1. Gestión y evaluación del riesgo

Grupo Fertiberia realiza de forma periódica un proceso de análisis y gestión de riesgos, que sirve como piedra angular de las actuaciones de seguridad. Este proceso permite conocer la situación de la seguridad y valorar los riesgos a los que están sometidos los activos de información.

Para la realización del análisis de riesgos, Grupo Fertiberia identifica las amenazas a las que están sometidos los activos, determinando la posibilidad de que dichas amenazas se materialicen. En función de este riesgo y del valor del activo, se determina el impacto o perjuicio de que ocurra una determinada situación en caso de materializarse una amenaza.

Junto con el análisis de riesgos, se realiza también un análisis de impacto, donde Grupo Fertiberia con los resultados de ambos planifica la gestión y el tratamiento de los riesgos identificados, seleccionando las salvaguardas necesarias para reducir los riesgos a unos niveles aceptables y de esta forma, reducir el impacto.

5.2. Políticas y Requisitos de Conformidad de la Seguridad

5.2.1. Aspectos organizativos de la seguridad de la información

Grupo Fertiberia dispone de una estructura organizativa de seguridad con el fin de coordinar y aprobar todos los aspectos relacionados con la Seguridad de la Información

Esta estructura organizativa está compuesta por:

Comité de Seguridad de la Información: El Comité de Seguridad de la Información coordina y centraliza todos los esfuerzos sobre las decisiones de seguridad, políticas, normas, análisis de riesgos, planes de continuidad de servicios, recuperación de desastres, etc. Se encarga, entre otras tareas, de aprobar la política, objetivos de seguridad, normas, análisis de riesgos, los planes de continuidad de servicios, etc. asegurando en todo momento la alineación con la estrategia de seguridad definida. En sus reuniones ordinarias se realiza la evaluación y revisión de la situación de Grupo Fertiberia respecto a la seguridad de la información y se estudian las propuestas de seguridad a abordar.

Responsable de Seguridad de la Información: Se responsabiliza entre otras tareas, de supervisar la implantación de las políticas, normas, guías, y procedimientos de seguridad establecidos en Grupo Fertiberia. Proporciona apoyo en materia de seguridad a todas las áreas de Grupo Fertiberia, realiza el seguimiento del estado de los incidentes de seguridad ocurridos, asegura el cumplimiento de las políticas, normas, guías, y procedimientos de seguridad, etc. Se responsabiliza de mantener y hacer cumplir la Norma de Funciones y Obligaciones en materia de Seguridad de la Información y Protección de Datos en colaboración con el Delegado de Protección de Datos cuando así proceda; además, en su caso, las derivadas de la normativa para la Protección de las Infraestructuras Críticas y de la Seguridad de las Redes y los Sistemas de la Información (normas PIC y NIS), más en concreto las de representación de Grupo Fertiberia ante el INCIBE-CSIRT Y CNPIC, órganos dependientes de la Secretaría de Estado de Seguridad, en coordinación con el Responsable de Seguridad y Enlace designado por Grupo Fertiberia para España y cuando proceda para Órganos Administrativos equivalentes en Francia y Portugal.

Propietarios de la Información: Son las personas responsables de la seguridad de cierta información, y los responsables de clasificarla en función de su confidencialidad, integridad y disponibilidad, designando las medidas de seguridad y los usuarios a los que se les permita el acceso a la información y la forma en que está es utilizada.

Custodios: Se responsabilizan de salvaguardar la información que les sea confiada por los propietarios, implementando las medidas de seguridad para proteger la información. Deben realizar copias de seguridad e implementar, operar y mantener las medidas de seguridad establecidas.

Usuarios que realicen tareas para Fertiberia (proveedores, subcontractados, personal en prácticas, etc.): Se responsabilizan de cumplir con las indicaciones establecidas en la Política de Seguridad de Grupo Fertiberia y en particular de:

- Conocer y aplicar las directrices y regulaciones en materia de seguridad de la información vigentes en el Proveedor de Servicios Digitales, haciendo un uso adecuado de la información y los sistemas que la soportan.
- No divulgar información de Grupo Fertiberia a personas no autorizadas.
- Utilizar los Sistemas de Información propiedad de Grupo Fertiberia para los fines designados, no permitiendo ni facilitando el uso de estos a personas no autorizadas.
- Utilizar contraseñas y códigos difíciles de adivinar y mantenerlos en secreto, evitando compartirlos o facilitarlos a otras personas.
- Reportar inmediatamente y siguiendo los procedimientos establecidos por Grupo Fertiberia cualquier evento que pueda comprometer la seguridad de su información o los Sistemas de Información que la soportan.
- Participar en las acciones formativas y planes relacionados con la seguridad de la información y protección de datos de carácter personal impartidas por Grupo Fertiberia.

5.2.2. Seguridad relativa a los RRHH.

Grupo Fertiberia tiene establecidas las medidas técnicas y organizativas necesarias para evitar los riesgos derivados de acciones humanas como pueden ser: fraude, sabotaje, robos, errores, etc.

Todos los usuarios tanto externos como internos, conocen y deben cumplir con las directrices de seguridad marcadas por Fertiberia para prevenir situaciones que puedan derivar en perjuicios, como pueden ser: pérdidas o usos indebidos de la información, deterioro o indisponibilidad de los sistemas, interrupción de los servicios prestados, etc.

5.2.2.1 Segregación de Tareas

Grupo Fertiberia es consciente de la importancia de la segregación de tareas en actividades consideradas como críticas y realiza las medidas que estima convenientes para evitar que una única persona disponga de plena capacidad para asumir todas las tareas en este tipo de actividad.

5.2.2.2 Formación y Concienciación

Según las necesidades identificadas, Grupo Fertiberia realiza las actividades de formación y concienciación por área, grupo o persona de destino.

El personal usuario de los servicios prestados por Grupo Fertiberia se responsabiliza de participar en las acciones formativas y de concienciación tanto en materia de seguridad de la información, como en materia de protección de datos de carácter personal, impartida por aquellas entidades designadas al efecto por los respectivos responsables en la materia.

5.2.2.3. Uso aceptable de los Sistemas de Información

Grupo Fertiberia, a través de los medios que crea oportunos, pone a disposición de todo el personal usuario, las pautas convenientes para realizar un buen uso de la información y de los sistemas que la soportan, con la finalidad de evitar riesgos derivados de su uso incorrecto o inadecuado.

5.2.3. Gestión de activos

El inventario de activos en relación con la Seguridad de la Información junto con la asignación de los responsables de cada uno de los activos tiene la finalidad de establecer una adecuada gestión de estos.

Para una protección adecuada de la información de su propiedad, Grupo Fertiberia ha realizado su clasificación y protección con las medidas de seguridad establecidas en función de su confidencialidad concretada en el Procedimiento para la Protección y Gestión de la Información Sensible.

Todo el personal de Grupo Fertiberia está familiarizado con la clasificación realizada y sus procedimientos de seguridad asociados.

Si los activos de Grupo Fertiberia se depositan en otras dependencias bajo la confianza de un tercero, se deben tratar con las mismas medidas de seguridad que están establecidas en las dependencias de Grupo Fertiberia.

5.2.4. Control de accesos

El acceso a la información y los sistemas de Grupo Fertiberia se concede en base a la necesidad de conocimiento, permitiendo el acceso en función de la necesidad legítima de acceso a la información para el desempeño de las funciones de cada usuario.

Cualquier otro acceso no se permitirá, a no ser que sea aprobado explícitamente por el Responsable de Seguridad de la Información de Grupo Fertiberia.

- **Identificación**

Grupo Fertiberia asigna identificadores que permiten identificar y registrar a los usuarios de forma inequívoca y personalizada.

Todos los Sistemas de Información que lo permitan, son dotados de mecanismos de control de acceso lógico, para comprobar la identidad del usuario y garantizar el acceso único y exclusivamente al personal autorizado a acceder a la información.

- **Autenticación**

Los usuarios de los servicios prestados por Fertiberia tienen la obligación de seleccionar contraseñas fuertes o difíciles de adivinar, no debiendo almacenar o ubicar las mismas en medios legibles o fácilmente accesibles, ni compartirlas con otros usuarios.

El Responsable de Seguridad de la Información realiza y solicita las revisiones periódicas de los accesos y permisos de usuarios, para poder comprobar que sólo el personal autorizado accede a la información y que se cumple con las directrices de seguridad establecidas.

5.2.5. Seguridad física y del entorno

5.2.5.1. Áreas Seguras (CPD,s)

Para las áreas consideradas como críticas, Grupo Fertiberia realiza las especificaciones mínimas de seguridad, como pueden ser:

- Mecanismos de seguridad físicos
- Controles de entrada y salida
- Medidas frente amenazas externas
- Aislamiento de sistemas sensibles, etc.

Con este fin, se reducen riesgos derivados de accesos no autorizados o daños a los recursos de información.

Para asegurar la continuidad y la efectividad de los servicios, Grupo Fertiberia determina la necesidad de realizar mantenimientos correctivos y preventivos de los sistemas y sus suministros de tal forma, que se garantice su correcto funcionamiento y configuración, y se desarrollen las medidas de seguridad necesarias que permitan dar continuidad a los servicios en caso de fallo.

Grupo Fertiberia elabora una serie de pautas de seguridad a seguir por el personal dentro de las instalaciones con la finalidad de prevenir diversas situaciones de riesgo. Se establecen

procedimientos para la notificación de eventos que pudieran comprometer la seguridad de los Sistemas de Información.

5.2.5.2. Oficina y despachos

Grupo Fertiberia analiza las medidas de seguridad mínimas necesarias (vigilantes, cerraduras en puertas, armarios y cajoneras con llave, etc.) para prevenir accesos no autorizados a la información que esté ubicada en las oficinas y en los despachos de Grupo Fertiberia.

El personal de Grupo Fertiberia comprueba que todos los equipos están bloqueados o apagados, y que la información quede almacenada o protegida convenientemente de accesos no autorizados cuando estas dependencias sean abandonadas.

5.2.6. Seguridad de las operaciones

5.2.6.1. Gestión de cambios y Configuración

Grupo Fertiberia tiene establecidos los procedimientos y las medidas que son necesarias para la gestión de los cambios y las configuraciones que puedan surgir, asegurando que los mismos sean aprobados por sus responsables y se realicen de forma correcta y eficiente.

El uso de nuevos sistemas o aplicaciones cuentan con la aprobación del Comité de Seguridad de la Información de Grupo Fertiberia.

En el seguimiento realizado por el Comité de Seguridad, se contemplan las necesidades de recursos y prioridades de las distintas Áreas para su planificación.

5.2.6.2. Código Malicioso

El código malicioso como pueden ser los virus, gusanos, troyanos, spyware, etc. son programas que pueden ser creados para llevar a cabo finalidades como: recopilar información sensible sobre el usuario, controlar un equipo, dañar o inutilizar un equipo, modificar o eliminar datos, etc.

Como medida de protección, todos los sistemas de Grupo Fertiberia disponen de software antivirus instalado y actualizado.

Para prevenir el software malicioso, los usuarios se responsabilizan de tomar las precauciones necesarias, como pueden ser: no descargar, ejecutar ni abrir ficheros que provengan de fuentes desconocidas, no instalar software no autorizado, pasar el antivirus a los soportes que van a ser utilizados, etc., además de que sólo el antivirus no garantiza la seguridad.

Si un usuario sospecha de infección de virus, debe notificarlo según los procedimientos definidos por Grupo Fertiberia para que se tomen las medidas correspondientes.

5.2.6.3. Gestión de Soportes y Copias de Respaldo

Grupo Fertiberia tiene establecido un registro de entrada y salida de los soportes en función de su clasificación, de tal forma que pueda garantizar que se realiza de forma autorizada y controlada.

Dispone de espacios específicos (unidades compartidas, carpetas de red, etc.) para el almacenamiento de información del personal y usuarios de los que realizan las copias de seguridad y pruebas periódicas. Las copias de seguridad realizadas se almacenarán en ubicaciones externas como medida de seguridad.

Grupo Fertiberia dispone de procedimientos para la realización de pruebas y recuperación de los datos, siendo el Responsable de Seguridad de la Información el encargado de vigilar que se cumplan y se realicen según las pautas marcadas.

Los usuarios se responsabilizan de solicitar las copias de seguridad al personal de soporte correspondiente, teniendo en cuenta que, como regla general, no se debe almacenar información de carácter sensible localmente en los equipos.

Para garantizar la confidencialidad de la información que lo requiera, Grupo Fertiberia aplica mecanismos de cifrado de las copias de seguridad y los protege con mecanismos que garantizan que la información no pueda ser accedida por personas no autorizadas.

5.2.7. Seguridad de las comunicaciones

Grupo Fertiberia realiza las medidas necesarias para proteger y fortalecer sus redes y comunicaciones, implantando los procedimientos y controles de seguridad en función de la criticidad de la información o sistemas a proteger.

Tiene en cuenta la segmentación de la red y el uso de protocolos seguros de comunicaciones y ha elaborado las directrices para el uso de Internet y correo electrónico, de tal forma que su uso se limite a aquellos aspectos directamente relacionados con la actividad de Fertiberia, así como las responsabilidades propias del puesto de trabajo del personal.

De esta manera se garantiza la seguridad en la información que se transfiere dentro de la organización y con cualquier entidad externa.

5.2.8. Adquisición, desarrollo y mantenimiento de los Sistemas de Información

5.2.8.1. Segregación de entornos

Grupo Fertiberia realiza las medidas necesarias para que los entornos de desarrollo, pruebas y producción estén diferenciados, de tal forma que las pruebas y desarrollos se ejecuten de una forma segura y controlada antes de su paso a producción.

En caso de subcontratar o externalizar el servicio, los desarrollos y el material generado mientras se preste el servicio, se consideran propiedad de Grupo Fertiberia, asumiendo así los derechos legales de propiedad.

5.2.9. Relación con Proveedores

Grupo Fertiberia establece los mecanismos necesarios para asegurar la protección de los activos de la organización que puedan ser accesibles por los proveedores.

5.2.10. Gestión de incidentes de seguridad

Grupo Fertiberia dispone de los medios que son necesarios para que todo el personal conozca sus responsabilidades y las acciones a realizar en caso de identificar un incidente de seguridad.

Siguiendo las indicaciones proporcionadas por Grupo Fertiberia, el personal reporta inmediatamente a la persona designada en los procedimientos o en su defecto, a su Responsable directo o al Responsable de Seguridad de la Información, cualquier evento que pueda comprometer la seguridad de los Sistemas de Información de Grupo Fertiberia como pueden ser: daños por fuego, agua, fallos de suministros, robo, accesos no autorizados a los sistemas o a las instalaciones, averías o irregularidades en las operaciones, suplantación de identidad, ataques, virus, etc.

Grupo Fertiberia realiza la gestión de los incidentes de seguridad de tal forma, que sea posible analizar y evaluar las causas y sus consecuencias y realizar las acciones correctivas o preventivas necesarias a la mayor brevedad posible y se acoge al plan de autoprotección del edificio donde están localizados.

5.2.10.1. Monitorización y Auditoría

Los registros de auditoría contienen la información necesaria para garantizar la trazabilidad de las actividades no permitidas que se encuentran fuera de los procedimientos establecidos.

Grupo Fertiberia realiza la monitorización y gestión de eventos de todos los procesos y sistemas que lo permitan para facilitar la realización de auditorías y revisiones de acceso y uso, pudiendo comprobar así el cumplimiento con la política, directrices, leyes y regulaciones aplicables, así como verificar el correcto funcionamiento de controles o salvaguardas de seguridad que se implanten.

Grupo Fertiberia realiza revisiones y auditorías tanto externas como internas para verificar el cumplimiento de las directrices de seguridad existentes e identificar las acciones correctivas, preventivas y de mejora necesarias.

Todos los contratos celebrados con proveedores y externos contemplan la necesidad de incluir cláusulas de *auditabilidad* que permiten a Grupo Fertiberia verificar el cumplimiento con las normas de seguridad dispuestas.

5.2.11. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

Grupo Fertiberia dispone de un proceso de gestión de la continuidad de sus servicios basado en los resultados del Análisis de Riesgos, de tal forma que los posibles fallos o interrupciones de los servicios afectados se puedan reducir a unos niveles aceptables.

El proceso de gestión de la continuidad de sus servicios incluye los controles para identificar y reducir los riesgos, limitar las consecuencias de incidentes y asegurar la reanudación a tiempo de las operaciones esenciales.

Para los servicios considerados como críticos, Grupo Fertiberia desarrolla y prueba regularmente planes de contingencias, teniendo en cuenta los procedimientos y recursos de respaldo que permiten una restauración efectiva y eficiente de los servicios afectados.

5.2.12. Cumplimiento

Grupo Fertiberia identifica y mantiene actualizada la relación de requisitos legales a aplicar en materia de seguridad de la información.

De esta forma se incluyen en los contratos, licencias y acuerdos establecidos en Grupo Fertiberia el cumplimiento con las normas de seguridad, cláusulas relativas a la propiedad intelectual, derechos de explotación, protección de datos de carácter personal, confidencialidad y no divulgación y requerimientos de seguridad exigibles por imperativos legales o regulatorios que sean de aplicación.

Grupo Fertiberia, en cumplimiento con los requisitos legales y regulatorios vigentes, asegura la confidencialidad, integridad y disponibilidad de los registros que pudieran ser requeridos por motivos legales y los protege frente a posibles pérdidas, destrucción o modificación.

Para cumplir con la protección de datos de carácter personal, acorde a la normativa regulatoria de la Unión Europea y sus desarrollos en España, Francia y Portugal, Grupo Fertiberia dispone tanto de una Política de Protección de Datos de Carácter Personal, como de una Política de Puesto de Trabajo Despejado ya aprobadas por los respectivos órganos de administración de todas las entidades que conforman Grupo Fertiberia, Delegado de Protección de Datos en España, Francia y Portugal, y un registro de actividades de tratamiento que es gestionado por cada Delegado de Protección de Datos -donde se identifican los ficheros que contienen datos de carácter personal, el responsable de cada fichero, su ubicación y nivel de protección asociado. Asimismo, en materia de protección de datos de carácter personal es de aplicación la Norma de Funciones y Obligaciones en materia de Seguridad de la Información y Protección de Datos.

Para asegurar el cumplimiento con todos los requisitos de seguridad, el Responsable de Seguridad de la Información, con la colaboración del Delegado de Protección de Datos de ser necesario, realiza revisiones técnicas y de cumplimiento de forma periódica, estableciendo las medidas de seguridad necesarias y generando los informes necesarios para su revisión en las reuniones con el Comité de Seguridad de la Información.