NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Índice

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

1 Introducción

1.1 Objeto

Este documento se ha redactado con el objetivo de establecer las directrices y principios generales para iniciar, adoptar, mantener y mejorar la seguridad de la información en el Grupo PLANASA y, para ello, se incluyen las medidas de seguridad aplicables a la información y sistemas de la información.

Con estas directrices se pretende establecer un punto de partida común y un marco para el desarrollo progresivo de los procedimientos necesarios, teniendo en cuenta las necesidades específicas en lo que respecta a la seguridad de la información.

Las necesidades específicas de la Organización pueden deberse a factores tales como la estructura organizativa, los procesos empresariales, los sistemas de información e, incluso, la ubicación geográfica.

Estas directrices se basan en normas y estándares internacionales de buenas prácticas para la gestión de la seguridad de la información.

Esta normativa cumple con los principios de información definidos por las Sedes del Grupo PLANASA en España.

1.2 Ámbito de aplicación

Este documento resulta de aplicación a todas las entidades que formen parte del Grupo PLANASA.

La adopción de estas directrices se realizará de forma que se respeten cualesquiera otros requisitos legales o internos que también puedan aplicarse para regular aspectos en los que coincidan.

Todos los trabajadores y terceros que tengan acceso a la información del Grupo PLANASA deberán conocer estas directrices.

1.3 Referencias

- Política de seguridad de la información del Grupo PLANASA.
- El Código ISO/IEC 27002:2005 de prácticas para la gestión de la seguridad de la información.
- Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT®) de ISACA
- La Biblioteca de Infraestructura de Tecnologías de Información (ITIL)
- Ley orgánica 15/1999 de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.
- RGPD (Reglamento General de Protección de Datos). Reglamento (UE) 2016/679

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

2 Definición de seguridad de la información

La información es un activo valioso y esencial para el Grupo PLANASA indispensable para el desarrollo de las actividades de la Organización.

La seguridad de la información se define como la protección de la confidencialidad, disponibilidad e integridad de la información respecto de una serie de amenazas para garantizar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de la inversión y las oportunidades.

Por ello, se reconoce la importancia de las medidas de seguridad para garantizar que la información no se vea afectada por amenazas internas y externas, tales como errores humanos, actos malintencionados (fraude, malversación, sabotaje, infracciones de privacidad, etc.), errores técnicos o eventos de fuerza mayor, como desastres naturales.

Los firmantes de esta Normativa son responsables de desarrollar, revisar y validar las políticas de seguridad.

La adopción de estas directivas por parte del Grupo PLANASA minimiza los posibles riesgos a los que está expuesta la Organización en el transcurso de sus actividades empresariales.

3 Organización de la seguridad

3.1 Responsabilidades

Se definirán de forma clara todas las responsabilidades con respecto de la seguridad de la información. Las personas a las que se haya asignado responsabilidades podrán delegar parte de sus tareas, pero seguirán siendo responsables de la correcta ejecución de las mismas.

A continuación se describen las principales responsabilidades en materia de seguridad de la información en el Grupo PLANASA.

3.1.1 Consejo de PLANASA

El Consejo de PLANASA fomenta de manera activa la seguridad de la información en todas las empresas que forman parte del Grupo, promoviendo acciones para mejorar la seguridad de la información. Además, el Consejo de PLANASA se compromete a:

- Facilitar directrices claras y apoyo visible a las iniciativas de seguridad de la información.
- Fomentar la adopción de medidas relativas a la seguridad de la información.
- Facilitar los recursos necesarios para garantizar el nivel adecuado de seguridad de la información.
- Aprobar el nombramiento de cargos y responsabilidades específicos para velar por la seguridad de la información en el conjunto de la Organización.
- Impulsar planes y programas relativos a la concienciación en materia de seguridad de la información.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

- Garantizar el cumplimiento de las normativas existentes en este ámbito de responsabilidad.
- Designar al Departamento de Sistemas de la Información para dirigir la adopción de esta Política en el Grupo PLANASA.

3.1.2 Comité de Seguridad de la Información

El Grupo PLANASA dispondrá de un Comité de Seguridad de la Información liderado por el Departamento de Sistemas que tendrá como objetivos principales:

- Desarrollar y mantener la Normativa de Seguridad de la Información del Grupo PLANASA.
- Proponer, fomentar y coordinar, a nivel de Grupo, todos los proyectos relativos a la seguridad de la información.
- Garantizar el cumplimiento de las políticas y directrices en materia de seguridad de la información para definir Planes de Gestión de Seguridad y Planes de Recuperación tras Desastres para los sistemas de información.
- Dirigir y coordinar el desarrollo y adopción de los procedimientos operativos necesarios en cuestión de seguridad de la información.
- Dirigir y coordinar la gestión del conocimiento en el Grupo PLANASA, trabajando en conjunto con los cargos corporativos y los expertos los ámbitos relacionados con la seguridad de la información.
- Coordinar acciones para mejorar la seguridad con el responsable para el cumplimiento de la ley local de protección de datos.

El Comité de Seguridad de la Información estará compuesto por representantes de las siguientes especialidades:

- Sistemas de la información
- Recursos Humanos
- Finanzas
- Cumplimiento

3.1.3 Director/ responsable de Seguridad de la información

La función de responsable de seguridad de la información se asignará al director de Tecnologías de la Información.

Entre las responsabilidades del director de Seguridad de la Información se incluyen:

- Definir y adoptar controles que cumplan con las políticas de seguridad de la información de la Organización.
- Coordinar los esfuerzos por evaluar la conveniencia de los controles adoptados y recomendar medidas adicionales a partir de dichas evaluaciones.
- Proponer mejoras de las metodologías y procesos de evaluación (por ejemplo, evaluación del riesgo) sujetas a la aprobación de la dirección.
- Evaluar los datos de gestión de incidentes de seguridad de la información en la organización e informar de dichos datos al responsable correspondiente, recomendado acciones adecuadas en función de los datos.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

- Identificar cambios significativos en las amenazas y vulnerabilidades, tanto a nivel interno como externo, y recomendar acciones apropiadas.
- Prestar servicios de asesoramiento para la seguridad de la información en la Organización.
- Controlar el nivel de seguridad de la información mediante los indicadores establecidos y la realización de auditorías.

El responsable de Seguridad de la Información podrá delegar parte de sus responsabilidades en otras personas bajo su supervisión.

3.1.4 Responsable de la protección de datos personales

En el contexto de la seguridad de la información, el responsable de la protección de datos personales definirá las obligaciones y requisitos jurídicos en materia de protección de datos personales para cumplir con la legislación en vigor.

Asimismo, el responsable de la protección de datos personales formará parte del Departamento de Recursos Humanos.

3.1.5 Responsable de procesos

El responsable de procesos es el encargado de garantizar que un proceso empresarial sea adecuado para un determinado fin.

Entre las responsabilidades del responsable de procesos se encuentran el respaldo, diseño y mejora continua de los procesos y parámetros.

Entre las responsabilidades del responsable de procesos en materia de seguridad de la información se incluyen:

- Asignar una clasificación apropiada a la información.
- Asignar responsabilidades administrativas y operativas cotidianas dentro del proceso.
- Determinar los criterios apropiados para acceder a la información y a los sistemas de la información (definición de funciones) y aprobar las solicitudes de acceso al sistema.
- Garantizar que los usuarios que participan en los procesos empresariales adoptan los controles de seguridad razonables y apropiados para proteger la confidencialidad, integridad y disponibilidad de la información.
- Comprender y aprobar los métodos de almacenamiento, tratamiento y comunicación de información por parte de la Organización.
- Definir la tolerancia al riesgo y aceptar o rechazar riesgos vinculados a las amenazas de seguridad que repercutan en la confidencialidad, integridad y disponibilidad de la información.
- Definir una estrategia de registro de auditorías (identificar los eventos que deben auditarse, definir las responsabilidades y frecuencia de las revisiones de los registros de auditoría, determinar los periodos de conservación de registros de auditoría, seguimientos, informes de auditoría, etc.).
- Comprender los efectos de las políticas y normativas de la Organización, contratos con terceros y requisitos legales sobre la información.

- Validar y aprobar cualquier cambio que pudiera repercutir de manera significativa en los procesos empresariales.

3.1.6 Usuarios

Cualquier persona a nivel interno o externo (trabajadores del Grupo PLANASA o personal externo) que utilice la información y los sistemas de información necesarios debe prestar la atención necesaria y cumplir con la Política de Seguridad de la información del Grupo PLANASA. Sus responsabilidades principales son:

- Utilizar los sistemas de la información únicamente para realizar tareas autorizadas en cumplimiento con la legislación y la regulación.
- Proteger la información a lo largo de su ciclo de vida desde la creación o recepción mediante el procesamiento, comunicación, transporte, almacenamiento, notificación a terceros o posible destrucción.
- Proteger cualquier tipo de información, informatizada o no, de forma acorde con las normativas de seguridad.
- Proteger la información frente accesos no autorizados, publicación indebida o pérdida.
- Conocer los requisitos legales y normativos de la Organización.
- Cualquier incumplimiento de las normativas de seguridad de la información deberá comunicarse de manera adecuada cuando se detecte.

3.2 Relaciones con terceros

Mediante la adopción de controles y la inclusión de cláusulas contractuales, el Grupo PLANASA garantizará que se mantiene la seguridad de la información en aquellos casos en los que se produzca el acceso, comunicación o tratamiento de datos por parte de terceros.

Para ello, es necesario identificar los riesgos asociados a la información y sistemas en los procesos empresariales en los que participen terceros para poder adoptar los controles apropiados antes de conceder acceso.

En aquellos casos en los que resulte necesario conectar con terceros, será preciso realizar previamente un proceso de evaluación de riesgos para poder identificar los requisitos de controles específicos.

Además, en los contratos con terceros se incluirán requisitos de confidencialidad y acuerdos de confidencialidad, así como acciones necesarias una vez se haya finalizado el contrato, tales como la devolución o destrucción de la información.

Los responsables de la contratación de terceros deberán garantizar que en dichos acuerdos se incluyan requisitos de seguridad de la información dependiendo del tipo de empresa y servicio prestado, en especial en los casos en los que el servicio implique el acceso, tratamiento, comunicación o gestión de información y sistemas de la información del Grupo PLANASA.

3.3 Auditoría de la seguridad de la información

Se realizará una revisión independiente y frecuente de la gestión de la seguridad de la información o cuando se introduzcan cambios significativos en materia de seguridad. Esta

revisión o auditoría podrá ser interna o externa, siempre y cuando se realice por una unidad independiente de la unidad objeto de auditoría.

4 Clasificación y gestión de activos

4.1 Responsabilidades respecto de los activos

El Grupo PLANASA garantizará el establecimiento de responsabilidades respecto de los principales activos de la Organización para garantizar y mantener una protección adecuada de los mismos.

A los efectos previstos en este documento, los activos podrán ser de varios tipos, pero todos ellos tienen valor para la Organización y forman parte de sus procesos empresariales:

- Activos de información: bases de datos, archivos, contratos y acuerdos, procedimientos operativos, información archivada, etc.
- Activos de software: aplicaciones, sistemas operativos, etc.
- Activos físicos: equipos informáticos, dispositivos de comunicación, equipo auxiliar, dispositivos extraíbles, etc.
- Suministros: electricidad, aire acondicionado, líneas de comunicación, etc.

Se identificarán y clasificarán todos los activos de la Organización y se les asignará un responsable. El responsable deberá garantizar que los activos se clasifiquen de manera correcta en el inventario y revisará esta clasificación cuando se produzcan cambios; además, garantizará que se cumplan los controles de seguridad identificados por la Organización.

El Grupo PLANASA garantizará que, además de identificar todos los activos importantes, se evalúe su criticidad, proceso en el que deberán participar todas las unidades de negocio.

En el inventario de activos del Grupo PLANASA se incluirá toda la información necesaria para la recuperación ante desastres, como: tipo de activo, formato, ubicación, información de copias de seguridad, licencias y su valor desde el punto de vista del negocio.

El Grupo PLANASA garantizará que se definan normas para el uso aceptable de la información y de los sistemas de la información, que se documentarán y adoptarán.

Todos los usuarios (trabajadores, socios externos y terceros) que tengan acceso a la información del Grupo PLANASA deberán conocer los usos permitidos. Algunas de las normas que deben conocer los usuarios son:

- Cuando se asigna y entrega un ordenador, dispositivo móvil o periférico a un usuario, este es responsable del mismo y no puede intercambiárselo con otros usuarios. El usuario responsable de un dispositivo determinado no permitirá el uso de su dispositivo sin supervisión, salvo al personal técnico que realice labores de mantenimiento y soporte.
- Cualquier cambio en la configuración inicial del equipo puede poner en peligro la seguridad de los datos, perjudicar los accesos a las comunicaciones y alterar su funcionamiento correcto, por lo que queda prohibido modificar la configuración inicial del

equipo. Además, los ordenadores y dispositivos móviles deberán conectarse a la red de la Organización con regularidad para que puedan actualizarse correctamente.
- Cuando se presten ordenadores, dispositivos móviles o periféricos, deberá establecerse una fecha de devolución. Los equipos deberán devolverse con todos sus componentes.
- Los robos o pérdidas de ordenadores, dispositivos móviles, unidades de almacenamiento de datos o documentación impresa deberán notificarse de forma inmediata.

4.2 Clasificación de la información

El Grupo PLANASA dispondrá de un documento de clasificación de la información que, dependiendo del tipo de información, permita establecer los controles apropiados para el uso y procesamiento de la información. La información de la Organización se etiquetará y protegerá de acuerdo con esta clasificación.

Se considerarán los siguientes niveles para clasificar la información:

- Pública
  - Este tipo de información puede comunicarse sin restricciones y está destinada para su uso por parte del público general.
  - En caso de hacerse públicos, estos datos no perjudicarían a ningún individuo, grupo ni a la Organización.
  - Precisa protección básica frente a manipulaciones no autorizadas. Este tipo de información puede compartirse libremente.
- Uso exclusivo interno
  - La información que no se etiquete como «Confidencial» se clasificará como de «Uso exclusivo interno».
  - Esta información puede comunicarse a trabajadores o terceros que guarden relación con la Organización, son sujeción a un acuerdo de confidencialidad previo.
  - Precisa protección frente a accesos o manipulaciones no autorizados.
- Confidencial
  - En caso de hacerse públicos, estos datos perjudicarían a algún individuo, grupo o a la Organización.
  - Precisan el mayor nivel de protección frente a accesos no autorizados, publicación o manipulación, en formato físico o electrónico.
  - Los responsables de procesos deben gestionar de manera meticulosa el acceso y almacenamiento de la información confidencial.
  - Únicamente se concederá acceso a dicha información a individuos que deban conocerla.

Pueden definirse subniveles de clasificación adicionales si resulta preciso siempre y cuando se incluyan, como mínimo, los tres niveles anteriores.

Todo el personal debe estar familiarizado con la clasificación y los procedimientos de seguridad asociados.

En caso de que los activos del Grupo PLANASA se depositen en instalaciones de terceros, deberán tratarse con las medidas de seguridad que establece el Grupo PLANASA.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

En el supuesto de que el personal del Grupo PLANASA tuviese acceso a información de terceros, esta se gestionará con las mismas medidas de seguridad que se apliquen a la información confidencial de la Organización.

Con respecto de la protección de datos de carácter personal, el Grupo PLANASA se guiará por las normativas y legislación locales.

5 Seguridad en materia de Recursos Humanos

El Grupo PLANASA garantizará que se disponga de los controles en materia de Recursos Humanos necesarios para reducir el riesgo de robo, fraude o uso indebido de información por parte de trabajadores, contratistas y terceros.

Se considerarán los siguientes aspectos con respecto de aquellos usuarios que desempeñen una función vinculada a la seguridad de la información:

- Contratación:
  - Evaluación previa a la contratación: se realizarán pruebas adecuadas para verificar la trayectoria de los candidatos (se incluirán, según proceda, componentes tales como verificación de la identidad, referencias, verificación de CVs, etc.).
- Durante la relación laboral
  - Condiciones laborales: el usuario firmará una declaración de condiciones laborales y derechos y responsabilidades con respecto de la seguridad de la información.
  - Concienciación, educación y formación respecto de la seguridad de la información: se ofrecerá al usuario formación en materia de seguridad de la información y actualizaciones frecuentes de las políticas y procedimientos de la organización.
  - Procedimiento disciplinario: deberá disponerse de un procedimiento disciplinario formal aplicable a aquellos que infrinjan la seguridad.
- Finalización:
  - Devolución de activos: la información y activos físicos de la Organización deberán devolverse una vez finalice la relación laboral o contractual.
  - Eliminación de derechos de acceso: deberán eliminarse los derechos de acceso a la información y a sistemas de la información una vez finalice la relación laboral o contractual.
  - Transferencia de conocimientos: se establecerán los mecanismos adecuados para garantizar que los conocimientos que se obtengan en el transcurso de la relación laboral permanezcan en la Organización una vez finalice la relación laboral o contractual.

El Grupo PLANASA garantizará que el personal y los terceros conozcan sus responsabilidades en materia de seguridad de la información. Para ello, será necesario desarrollar normas en las

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

que se detallen las responsabilidades, deberes y obligaciones de los usuarios en lo que respecta a seguridad de la información.

En estas normas se regulará, al menos:

- Los usos permitidos de los sistemas de la información.
- El uso de identificadores y contraseñas.
- La obligación de confidencialidad.
- El cumplimiento de la legislación (normativas en materia de protección de datos de carácter personal, propiedad intelectual, etc.).

Para determinados perfiles con mayores responsabilidades con respecto de la seguridad de la información, sus funciones y deberes se documentarán de manera adecuada y se comunicarán formalmente a las personas a las que se asignen dichas funciones.

El Grupo PLANASA garantizará la separación de tareas en procesos críticos, adoptando las medidas necesarias para evitar que una única persona tenga capacidad para desempeñar todas las tareas en este tipo de procesos.

Asimismo, la Dirección de Recursos Humanos deberá establecer mecanismos para:

- Comunicar de forma adecuada las normas y normativas de seguridad de la información al personal afectado.
- Solicitar a los trabajadores que firmen cláusulas de confidencialidad cuando resulte recomendable y viable.
- Recordar con frecuencia a los trabajadores sus responsabilidades con respecto de la seguridad de la información.
- Educar a los trabajadores en cuestiones relacionadas con la protección de información corporativa sensible mediante acciones de formación y concienciación.
- Limitar el acceso a archivos o ubicaciones que contengan información sensible.
- Evitar facilitar información confidencial sobre la Organización durante los procesos de contratación y selección.
- Emprender las medidas apropiadas para evitar o limitar la pérdida de información cuando un trabajador abandona la Organización, dependiendo del nivel de acceso a información sensible que tuviera (por ejemplo, realizar entrevistas antes de su salida y revocar derechos de acceso).
- Identificar a aquellos que trabajen con información sensible, bien sean trabajadores, consultores o socios externos y controlar, como medida preventiva, su acceso a la información con el nivel de detalle y frecuencia que se considere apropiado según la naturaleza de la información.

Con respecto de la protección de datos de carácter personal, la Dirección de Recursos Humanos se guiará por las normativas y legislación locales.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

6 Seguridad física y ambiental

El Grupo PLANASA garantizará que se establezcan los mecanismos apropiados para evitar accesos físicos no autorizados y posibles daños a las instalaciones o equipos de la Empresa.

Será necesario definir un nivel de seguridad para cada área (centros de datos, oficinas, etc.) y que se adopten los controles adecuados para cumplir con, al menos, los siguientes aspectos:

- Autorización adecuada para el personal al que deba concederse acceso a zonas restringidas.
- Definición de perímetros de seguridad (como barreras físicas, controles de acceso con tarjeta, mostradores de recepción vigilados, etc.) para controlar el acceso a las instalaciones.
- Diseño y aplicación de mecanismos de protección física ante daños como incendios, inundaciones, terremotos u otros tipos de desastres naturales o antrópicos.
- Control de las zonas de carga y descarga y, cuando sea posible, aislamiento de estas zonas de los recursos de tratamiento de información para evitar accesos no autorizados.
- Uso de sistemas de detección de intrusos, como alarmas de movimiento y perímetro o vigilancia de audio o vídeo.
- Establecimiento de controles de acceso adecuados para garantizar únicamente el acceso de personal autorizado.
    - Registro de la fecha/ hora de entrada y salida de visitantes o grabación en vídeo de la actividad en la zona de entrada/ salida, según proceda.
    - Todos los trabajadores, contratistas y visitantes deberán llevar su tarjeta de identificación visible en todo momento.
- Se protegerá de manera especial las zonas con recursos de procesamiento de la información.
    - Los derechos de acceso a estas instalaciones se revisarán, actualizarán y revocarán según proceda.
    - Será posible obtener un registro de auditoría de todos los accesos a dichas instalaciones.

Con respecto de la seguridad de los equipos, se efectuarán los siguientes controles:

- Los equipos se colocarán y protegerán de forma que se reduzcan los riesgos de amenazas medioambientales y las posibilidades de accesos no autorizados.
- Los equipos deberán estar protegidos frente a fallos de potencia, telecomunicaciones u otras alteraciones causadas por fallos en los servicios de soporte.
- El tendido eléctrico y las líneas de transmisión de comunicaciones de los sistemas de la información se protegerán contra interceptación o daños.
- Los equipos se conservarán de manera adecuada para garantizar su disponibilidad e integridad.
- Deberán aplicarse medidas de seguridad apropiadas para los equipos que se encuentren fuera de las instalaciones.
- No deberán retirarse los equipos, información o *software* de las instalaciones sin autorización previa y en virtud de las restricciones correspondientes

- Se aplicarán controles de seguridad en el traslado de equipos y aquellos que se encuentren fuera de las instalaciones adecuados a la configuración y sensibilidad de la información del dispositivo.
- Los equipos que contengan medios de almacenamiento y dispositivos de almacenamiento independientes deberán revisarse para garantizar que se hayan eliminado o sobrescrito de forma segura los datos sensibles y *software* bajo licencia antes de su eliminación o reutilización.

7 Gestión de comunicaciones y operaciones

7.1 Procedimientos y responsabilidades operativas

Se documentarán y actualizarán tanto los procedimientos operativos como las buenas prácticas del Grupo PLANASA y estarán disponibles para todos los usuarios que los necesiten para el desarrollo de sus funciones. Para ello, el Grupo PLANASA garantizará que esta documentación se revise con carácter periódico y que coincida con las versiones más actualizadas de las directrices en las que se base.

Según proceda, se separarán las tareas y responsabilidades para reducir las posibilidades de que se produzcan modificaciones o usos indebidos de los activos de la organización.

7.2 Gestión de servicios de terceros

El Grupo PLANASA garantizará que se incluyan controles de seguridad de la información, definiciones de servicios y especificaciones del nivel de servicio en los contratos de prestación de servicios con terceros.

El departamento responsable de un servicio de terceros garantizará la comunicación efectiva de las políticas de seguridad de la información, normativas y procedimientos del Grupo PLANASA al personal de terceros y mantendrá un control y revisión continuos de los servicios de terceros para garantizar el cumplimiento de los requisitos establecidos.

7.3 Planificación y aceptación de sistemas

El Grupo PLANASA garantizará que se controle el uso de la información y de los sistemas de la información para identificar y planificar requisitos de capacidad futuros, teniendo en cuenta el uso actual, tendencias esperadas y cambios previstos en los requisitos de negocio.

Asimismo, los criterios de aceptación de nuevos sistemas de la información, actualizaciones y nuevas versiones se establecerán de manera adecuada y se realizarán pruebas adecuadas durante su desarrollo o antes de su aceptación.

7.4 *Software* malicioso

Código malicioso, como virus, gusanos, troyanos, *spyware*, etc. son programas que pueden crearse para fines como: recopilar información sensible, controlar un ordenador, dañar o desactivar un ordenador, modificar o eliminar datos, etc.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

El Grupo PLANASA garantizará que se adopten controles para la detección, prevención y recuperación de *software* malicioso y que se establezcan procedimientos para concienciar a los trabajadores.

7.5 Navegación en Internet y mensajería electrónica

Los usuarios del Grupo PLANASA podrán recibir acceso a Internet y a mensajería electrónica. La mensajería electrónica comprende correo electrónico, mensajería instantánea (MI), conferencias de vídeo y audio y otras comunicaciones individuales o múltiples.

El Grupo PLANASA garantizará que la información que se utilice en la navegación en Internet y mensajería electrónica se proteja de forma adecuada.

Entre las medidas y procedimientos de seguridad en lo que respecta a la navegación en Internet y mensajería electrónica se incluye:

- Protección de los mensajes frente a accesos no autorizados, modificaciones o desviaciones.
- Direccionamiento y enrutamiento correcto.
- Fiabilidad y disponibilidad de los servicios de Internet y mensajería.
- Limitaciones en el uso de sistemas de mensajería menos seguros (como correos gratuitos/ comerciales y MI).
- Mayores niveles de identificación y protección del contenido de los mensajes cuando se utilicen redes públicas.
- Herramientas de filtrado web para evitar el acceso a contenido inapropiado (pornografía, apuestas, piratería, intervención de códigos informáticos, etc.).
- Restricciones en el tipo de archivos intercambiados para reducir el riesgo de que se produzcan infecciones de virus y uso no razonable de sistemas (por ejemplo, archivos ejecutables, audio y vídeo, etc.).
- Correo masivo, spam y técnicas de detección de robo de identidad.

7.6 Copia de seguridad de la información

El Grupo PLANASA garantizará que se realicen copias de seguridad de la información y del *software* y que se prueben en intervalos apropiados, de conformidad con la política de copias de seguridad acordada. El objetivo consiste en poder mantener la integridad y disponibilidad de la información y de los sistemas de información.

Las normas y procedimientos de copias de seguridad deberán incluir, al menos, los siguientes aspectos:

- Definición formal del nivel de copia de seguridad necesario para cada sistema (alcance de los datos que deben copiarse, frecuencia, duración del almacenamiento, etc.) a partir de los requisitos legales, contractuales y empresariales.
- Cumplimentar la documentación relativa a los procedimientos de restablecimiento de cada sistema;
- Almacenar las copias de seguridad en ubicaciones remotas para garantizar que puedan recuperarse en caso de desastre.

- Probar de manera frecuente los dispositivos de copia de seguridad y procedimientos de restablecimiento.

En este sentido, se garantizará en todo momento el cumplimiento de las especificaciones de la legislación local en materia de protección de datos.

7.7 Seguridad de la red

El Grupo PLANASA garantizará que las redes de la Organización se gestionen y controlen de manera adecuada para protegerlas frente a amenazas y mantener la seguridad de los sistemas y aplicaciones conectados a la red y a la información en tránsito.

Se identificarán las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red y se incluirán en los acuerdos de servicio de red, tanto si estos servicios se prestan a nivel interno o externo.

7.8 Gestión de dispositivos de almacenamiento

El Grupo PLANASA establecerá procedimientos para la gestión de dispositivos para evitar la publicación, modificación, eliminación o destrucción no autorizada de activos de información o interrupciones de las actividades empresariales.

La eliminación o retirada de dispositivos de almacenamiento se realizarán de manera segura para evitar que se filtre información a terceros.

Se protegerá de forma adecuada la documentación para los sistemas de datos organizativos de accesos no autorizados, puesto que puede contener información sensible (descripciones de aplicaciones, procesos, estructuras de datos, etc.).

Para garantizar la confidencialidad, el Grupo PLANASA asegurará la adopción de mecanismos de cifrado de los dispositivos que contengan información sensible en ubicaciones de almacenamiento y durante el transporte.

7.9 Intercambio de información

El Grupo PLANASA garantizará que se desarrollen y adopten las medidas de control adecuadas para proteger el intercambio de información tanto dentro como fuera de la Organización, con independencia del tipo de instalación de comunicación y dispositivo de almacenamiento de datos.

Estas medidas de control deberán cumplir con los requisitos específicos de la ley local en materia de protección de datos de carácter personal.

En caso de que se produzcan intercambios de información o software entre la Organización y partes externas, se establecerán acuerdos en los que se incluyan, al menos, los siguientes aspectos:

- Procedimientos para asegurar la correcta identificación y etiquetado, que se notifique de manera adecuada al emisor y al receptor, trazabilidad y aceptación.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

- Requisitos técnicos mínimos de embalaje y transmisión.
- Especificación de responsabilidades en caso de que se produzca un incidente relativo a la seguridad de la información.
- Cualquier otro tipo de medida de seguridad que se considere necesario por el tipo de información.

Si el envío de información se efectúa mediante dispositivos de almacenamiento físicos, se establecerán medidas de seguridad apropiadas para evitar accesos no autorizados, usos indebidos o alteraciones durante el transporte. En estos controles deberá incluirse:

- La fiabilidad de los transportistas o servicios de correo, que deben ser aprobados por la unidad correspondiente.
- La identificación de los mensajeros que recogen los dispositivos.
- El uso de contenedores diseñados para proteger el contenido de daños físicos que pudieran producirse durante el transporte.

Si la información es sensible, el Grupo PLANASA considerará controles adicionales como el uso de contenedores cerrados, entrega en mano, detección de apertura de embalajes, cifrado de datos, etc.

El Grupo PLANASA garantizará que se establezcan y adopten procedimientos para proteger la información vinculada a la interconexión de sistemas de la información empresariales.

7.10 Trazabilidad

El Grupo PLANASA evaluará que se mantengan registros de auditoría para registrar las actividades de los usuarios y sistemas, excepciones y eventos de seguridad de la información; estos registros se revisarán y conservarán durante un periodo acordado para ayudar en futuras investigaciones y vigilancia de los controles de acceso.

El mantenimiento de registros de auditoría conllevará implicaciones desde el punto de vista de la protección de datos personales y de la privacidad de los individuos. Por ende, antes de mantener registros de auditoría, se tendrá en cuenta la legislación aplicable.

Se protegerá toda la información relativa a los registros de auditoría frente a cualquier manipulación o acceso no autorizado.

Se registrarán y analizarán las actividades de los administradores y operadores de sistemas, así como sus fallos y se tomarán medidas como parte del proceso general de auditoría.

Los relojes de todos los sistemas de procesamiento de información pertinentes se sincronizarán de manera adecuada con la fuente de tiempo acordada para proteger la precisión de la información de registro.

El Grupo PLANASA considerará los requisitos de registro de auditoría para cumplir con la ley local en materia de protección de datos de carácter personal.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

8 Control de accesos

8.1 Procedimientos de gestión de accesos

El Grupo PLANASA garantizará que se establezcan, documenten y revisen con frecuencia procedimientos de control de accesos según las necesidades empresariales y los requisitos externos. En los procedimientos de gestión de accesos y los controles asociados se tendrán en cuenta los siguientes aspectos:

- Requisitos de seguridad para la información y sistemas de la información de los procesos empresariales (dependiendo del tipo de información, amenazas previstas y vulnerabilidades, requisitos de confidencialidad, integridad y disponibilidad, etc.).
- Directrices para determinar los derechos de acceso, como el principio del menor privilegio (los usuarios únicamente tendrán acceso a la información necesaria para el ejercicio de sus funciones) o clasificación de la información (confidencial, de uso interno, etc.).
- Segregación de tareas durante la concesión de accesos (por ejemplo, solicitudes, autorizaciones o administración de accesos)
- Flujo de autorización para conceder accesos (la autorización deberá ser aprobada por el responsable directo del usuario, director del departamento, titular, etc.).
- Controles establecidos para la eliminación puntual de derechos de acceso.
- Requisitos legislativos y normativos relevantes (por ejemplo, ley local en materia de protección de datos de carácter personal).
- Coherencia entre dichos procedimientos en sistemas y redes.

8.2 Gestión de acceso de usuarios

El Grupo PLANASA garantizará que se definan procedimientos formales de registro y baja de usuarios para conceder y revocar el acceso a los sistemas y servicios de información. El uso y gestión de privilegios de accesos estará controlado y restringido.

El Grupo PLANASA garantizará que se establezcan controles para revisar los derechos de acceso de los usuarios. En estos controles deberá incluirse:

- Revisión periódica de los listados de usuarios (por ejemplo, cada seis meses), especialmente para roles privilegiados («superusuarios»).
- Revisión más frecuente de derechos de acceso privilegiados («superusuarios»).
- Revisión de los usuarios tras cualquier cambio de estado (promoción, descenso de categoría, transferencia, finalización, etc.).

Se establecerán mecanismos de identificación y autentificación para acceder a los sistemas mediante un nombre de usuario y contraseña.

Todos los usuarios del sistema dispondrán de un identificador único («ID de usuario») de uso exclusivo personal. Los ID de usuario únicamente se compartirán en circunstancias excepcionales, cuando haya una justificación evidente y con la autorización del propietario. En dichos casos, se activarán controles adicionales para garantizar la responsabilidad de las acciones emprendidas con dichos ID de usuario.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Se establecerán procedimientos formales de gestión de contraseñas para garantizar la confidencialidad y seguridad de las contraseñas. En estos procedimientos se incluirán métodos de seguridad para crear y distribuir contraseñas temporales e iniciales.

Las contraseñas se cambiarán de forma periódica y deberán cumplir los parámetros de seguridad mínimos, que los usuarios deberán conocer. En este sentido, el sistema de gestión de contraseñas deberá:

- Garantizar la calidad de las contraseñas y no permitir que se creen contraseñas que no cumplan el requisito mínimo de 8 caracteres (con letras, números y símbolos).
- Solicitar al usuario el cambio de contraseñas, al menos, cada 90 días.
- Mantener un registro de 3 contraseñas utilizadas para que los usuarios no puedan repetirlas.
- Almacenar contraseñas cifradas.

El acceso a los sistemas de la información del Grupo PLANASA estará protegido por procedimientos de acceso seguros. Para que un procedimiento de acceso se considere seguro:

- No debe mostrar mensajes de ayuda que puedan ayudar a usuarios no autorizados a acceder al sistema.
- No debe mostrar las contraseñas al escribir (por ejemplo, esconderlas con símbolos como asteriscos).
- No debe transmitir contraseñas como texto sin cifrar en la red.
- Debe limitar el número de intentos de acceso durante un periodo concreto.

El Grupo PLANASA considerará la posibilidad de bloquear sesiones inactivas una vez transcurrido un tiempo de inactividad determinado, dependiendo de la importancia de la información a la que se haya accedido o de los riesgos asociados a la ubicación del equipo. Para poder activar de nuevo la sesión será necesario volver a identificarse.

En el caso de aplicaciones de alto riesgo o comunicaciones remotas, el Grupo PLANASA considerará la posibilidad de establecer restricciones a los tiempos de conexión, tales como restringir la duración total de la conexión o el periodo de conexión (por ejemplo, horario de oficina normal); restringir las ubicaciones de conexión (por ejemplo, a un rango de direcciones IP) o solicitar que el usuario vuelva a identificarse una vez haya transcurrido un intervalo tiempo determinado.

Todos los usuarios de los sistemas de la información del Grupo PLANASA (tanto trabajadores como personal externo) deben conocer:

- Sus responsabilidades con respecto de la custodia, uso y creación de contraseñas, con especial atención a la naturaleza personal de las contraseñas o la prohibición de compartirlas.
- Las acciones que deben realizar cuando dejen sus ordenadores desatendidos, como cerrar la sesión.
- La obligación de mantener el escritorio y la pantalla ordenados, garantizando que la posible información sensible se almacene bloqueada, que los documentos se recojan inmediatamente de las impresoras y que se mantenga la custodia de la información a la que accedan en el marco de sus actividades laborales.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

8.3 Control de acceso a la red

En lo que respecta al uso de servicios de red, el Grupo PLANASA garantizará que se establezcan controles para garantizar que los usuarios únicamente tengan acceso a los servicios para los que estén autorizados específicamente. Asimismo, en la medida de lo posible, se restringirán las capacidades de conexión de los usuarios a las acciones necesarias para el desarrollo de sus funciones.

En las conexiones remotas (conexiones externas), se evaluarán los riesgos para determinar el método de identificación apropiado, teniendo en cuenta los siguientes aspectos:

- Análisis de la opción de identificar los ordenadores en red para identificar conexiones de ubicaciones o equipos específicos.
- Control y limitación de accesos (tanto físicos como lógicos) a los puertos de configuración y diagnósticos remotos. En aquellos casos en lo que no sean estrictamente necesarios en las actividades empresariales, se deshabilitarán.
- Evaluación de la conveniencia de separar determinados servicios o sistemas específicos en la red, aplicando a cada dominio medidas de seguridad apropiadas para responder al riesgo.
- Evaluación de la necesidad de enrutar mecanismos para garantizar que las conexiones de red entre máquinas y flujos de información no infrinjan la política de accesos.

8.4 Derechos de acceso privilegiados

El Grupo PLANASA garantizará que se adopten controles para restringir los accesos a los sistemas operativos y bases de datos a usuarios autorizados, solicitándose la identificación de los usuarios autorizados de conformidad con la política de control de accesos definida. Se registrará y controlará el uso de privilegios de sistema especiales.

El Grupo PLANASA garantizará que el uso de servicios del sistema que sean capaces de invalidar el sistema y los controles de acceso a la aplicación se restrinjan y se controlen de manera adecuada cuando se utilicen (por ejemplo, mediante procesos de registro especiales).

8.5 Control de accesos a aplicaciones y datos

Los sistemas del Grupo PLANASA permitirán controles de acceso lógicos coherentes con las normas de control de accesos definidas, de forma que los usuarios dispongan de acceso restringido conforme a estas normas.

Se evaluará la necesidad de aislar sistemas sensibles, es decir, establecer un entorno informático dedicado especialmente a aquellos sistemas que contengan información crítica o sensible.

8.6 Informática móvil y teletrabajo

El Grupo PLANASA garantizará que se definan directrices y procedimientos en los que se incluyan controles para trabajar con dispositivos de informática móvil (portátiles, tabletas, etc.) que contengan información de la Compañía. Se tendrán en cuenta los siguientes aspectos:

- Protección física del equipo (atención especial a posibles robos).

- Identificación de usuario apropiada y controles de acceso.
- Métodos de cifrado para el almacenamiento de datos sensibles.
- Copias de seguridad para el almacenamiento de datos sensibles.
- Antivirus y otros programas de protección.
- Seguridad para las conexiones de red.
- Normas para el uso de dispositivos portátiles en zonas públicas.

En los casos en los que se permita teletrabajar, el Grupo PLANASA garantizará que se definan directrices en las que se contemplen, al menos:

- Las autorizaciones necesarias para teletrabajar.
- Medidas de seguridad física y ambiental para el entorno en el que se vaya a teletrabajar.
- Propuesta de entorno de trabajo: equipo que debe utilizarse en el teletrabajo, soporte y mantenimiento.
- Requisitos de seguridad de las comunicaciones, dependiendo de la importancia de los recursos a los que se accederá de forma remota.
- Uso de redes domésticas y requisitos o restricciones de la configuración de redes inalámbricas.
- Protección antivirus y requisitos de *firewall*.
- Procesos de copias de seguridad y medidas de seguridad para dichas copias.
- Auditoría y revisión de seguridad.
- Revocación de autorizaciones, derechos de acceso y devolución de equipo una vez se hayan completado las actividades de teletrabajo.

9 Adquisición, desarrollo y mantenimiento de sistemas

En las solicitudes de nuevos sistemas de información o mejoras de los actuales por parte de las unidades de negocio del Grupo PLANASA se incluirán especificaciones con los requisitos de seguridad. La unidad de negocio que efectúe la solicitud deberá tener en cuenta la importancia de la información procesada por el sistema y de los procesos empresariales.

Cuando se adquiera o desarrolle un sistema, en la medida en que lo precise la importancia del sistema, se tendrán en cuenta los siguientes aspectos relativos a la aplicación de controles de procesos:

- Validación de datos de entrada.
- Validación de procesamiento interno.
- Requisitos de identificación e integridad de mensajes entre procesos.
- Validación de datos de salida.

Cuando se considere apropiado, dependiendo de los requisitos de la seguridad del sistema, se establecerán mecanismos de cifrado, garantizando que se identifiquen los controles necesarios en lo que respecta a:

- Normas del uso de cifrado.

- Gestión de claves cifradas.

El Grupo PLANASA garantizará que se adopten los controles apropiados durante la adquisición, desarrollo y mantenimiento de sistemas para garantizar la seguridad de los archivos del sistema, como:

- Entornos separados para el desarrollo, preproducción (si la hubiera) y producción, en la medida de lo posible, para reducir los riesgos de accesos no autorizados o cambios disruptivos en los sistemas de producción.
- Controles para la instalación de *software* en sistemas de producción.
- Protección de datos de prueba, en especial si contienen información sensible o información sujeta a la legislación en materia de protección de datos de carácter personal.
- Control de acceso al código fuente del *software*.

El Grupo PLANASA garantizará que la adopción de cambios en los sistemas de la información se documente y controle mediante el uso de procedimientos formales de cambio de control. Para ello, será obligatorio establecer mecanismos que garanticen que:

- Se disponga de procedimientos formales para la gestión del cambio, así como la especificación, autorización, prueba, aceptación de usuario e implantación controlada.
- Las modificaciones al paquete de *software* se restringirán en la mayor medida posible, limitándose a situaciones en las que haya una necesidad justificada.
- La Organización supervisa y controla de manera adecuada el desarrollo de software externalizado.
- Una vez implantados, se revisan y prueban los sistemas para garantizar que no se hayan producido efectos adversos.
- Se minimizan o evitan las oportunidades de que se filtre información.

Además, el Grupo PLANASA garantizará que se establezcan procedimientos para mantener actualizada la información publicada acerca de vulnerabilidades técnicas y garantizará que se apliquen las medidas correctivas apropiadas para hacer frente a los riesgos que entrañan dichas vulnerabilidades.

10 Gestión de incidentes

El Grupo PLANASA garantizará que se establezcan mecanismos de comunicación y resolución de incidentes, eventos y debilidades que se descubran respecto de la seguridad de la información.

Todos los usuarios de sistemas de la información del Grupo PLANASA (trabajadores, contratistas y terceros) deberán informar de incidentes de información que detecten o sospechen mediante los canales adecuados tan pronto como resulte posible.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Se establecerán de forma clara las responsabilidades y procedimientos de gestión de incidentes para garantizar una respuesta rápida, efectiva y ordenada de los incidentes de seguridad de la información.

El Grupo PLANASA garantizará que se establezcan mecanismos para cuantificar y controlar el tipo, volumen y coste estimado de los incidentes de seguridad de la información.

Una vez se haya resuelto por completo el incidente, se definirá un procedimiento de cierre para recopilar las conclusiones extraídas e iniciar acciones de mejora en caso de que fuese necesario.

En aquellos casos en los que resulte necesario emprender acciones legales contra una personal u Organización como resultado de un evento o incidente de seguridad de la información, deberá considerarse la legislación aplicable para la recopilación, tratamiento y presentación de pruebas a la autoridad competente.

11 Gestión de la continuidad empresarial

El Grupo PLANASA garantizará que se desarrollen y mantengan planes de continuidad empresarial y procedimientos en los que se aborden todos los procesos críticos de la Organización. En estos procedimientos se incluirán todos los requisitos de seguridad de la información necesarios para mantener o restablecer las operaciones y garantizar la disponibilidad de información en el nivel y momento necesario tras las interrupciones o fallos en los procesos empresariales.

En los procedimientos de continuidad empresarial se determinarán las acciones necesarias en caso de fallo en un proceso organizativo crítico. La evaluación de la continuidad empresarial deberá comenzar con la identificación de eventos que puedan causar interrupciones en los procesos empresariales, junto con la probabilidad de ocurrencia, la repercusión de dichas interrupciones y sus consecuencias para la seguridad de la información.

Los planes y acciones para garantizar la continuidad empresarial se basarán en análisis de procesos empresariales para identificar cuál de ellos son críticos y definir un Tiempo Objetivo de Restablecimiento (TOR, a qué velocidad deben recuperarse los procesos empresariales en caso de que se produzca un desastre importante) y un Punto Objetivo de Recuperación (POR, la pérdida de información que la Organización puede asumir dependiendo de la repercusión empresarial)

El Grupo PLANASA garantizará que, tanto para los sistemas de la información gestionados a nivel interno como los gestionados a nivel externo, se desarrollen Planes de recuperación ante desastres como complemento a los planes y procedimientos de continuidad empresarial.

En el supuesto de que la continuidad empresarial dependa de proveedores, el Grupo PLANASA incluirá Acuerdos de niveles de servicio adecuados para garantizar el TOR y POR.

Los planes y procedimientos de continuidad empresarial se probarán y actualizarán con regularidad para garantizar que están actualizados y son efectivos.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

12 Cumplimiento

12.1 Cumplimiento de los requisitos externos

El Grupo PLANASA será responsable de definir, documentar y actualizar todos los requisitos legales, regulatorios o contractuales que sean relevantes para los sistemas de la información, así como las acciones emprendidas por la Organización para su cumplimiento.

Para ello, se establecerán controles y responsabilidades específicos para cumplir con los requisitos existentes.

Algunos aspectos relevantes que deben tenerse en cuenta en materia de cumplimiento son:

- Cumplimiento de la legislación relativa al uso de material protegido por derechos de propiedad intelectual y de *software* con licencia.
- Protección de registros importantes de la Organización frente a pérdidas, destrucción o falsificación.
- Cumplimiento de ley local en materia de protección de datos de carácter personal.
- Si se utilizan mecanismos de cifrado, se garantizará que cumplen todos los requisitos establecidos en la legislación aplicada.

12.2 Cumplimiento de los requisitos internos

El Grupo PLANASA garantizará que la información y los sistemas de la información cumplen con la normativa vigente en lo que respecta a la seguridad de la información.

El Grupo PLANASA garantizará que se comuniquen de forma efectiva a todas las personas que guarden relación con la Organización (así como a partes externas relevantes que gestionen datos en nombre de la Organización), las políticas y normativas de seguridad de la información.

Los directores de las distintas unidades de negocio deberán garantizar que se desarrollen procedimientos de seguridad de la información de manera correcta en sus áreas de responsabilidad, garantizando el cumplimiento de las normativas y procedimientos de seguridad de la información.

Los sistemas de la información del Grupo PLANASA se revisarán con carácter periódico para verificar el cumplimiento de las medidas y controles de seguridad. Se planearán y ejecutarán auditorías de sistemas de la información para minimizar los riesgos de alteración de los procesos empresariales.

Se protegerá el acceso a las herramientas de auditoría para evitar posibles usos indebidos o alteraciones.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Aprobación

Elaborado por:	Aprobado por:	Fecha de aprobación:
Director global de Sistemas de la Información	**Junta directiva del Grupo Planasa**	**Febrero de 2020**