POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

soluciones
MADIVA

Control de modificaciones

Fecha	Autor	Versión	Referencia de cambios	Estado
30/07/2024	A2SECURE	1.0	Primera edición	Aprobado

Contenido

1. Introducción y objetivos

La seguridad de la información es un reto a tener en cuenta en la gestión del riesgo empresarial. La falta de protección adecuada y de gestión de los riesgos que afectan a la seguridad de la Información puede resultar en pérdidas financieras para Madiva, y tener un impacto en su marca y reputación.

La Política de Seguridad de la Información de Madiva establece requisitos de seguridad mínimos y concisos que la empresa debe satisfacer en sus entornos.

Esta política identifica los requisitos de protección de la información para asegurar que todos los departamentos protegen la información de la empresa siguiendo las mejores prácticas y normativa vigente. Esta política representa los mínimos requisitos en Seguridad de la Información que todos los departamentos de Madiva han de seguir.

Esta política de Seguridad de la Información está alineada con el estándar internacional **UNE-EN ISO/IEC 27001:2022** "Seguridad de la información, ciberseguridad y protección de la privacidad".

1.1 Normativa interna relacionada

- Procedimiento de Gestión y Notificación de Brechas de Seguridad
- Procedimiento de gestión de excepciones a la Política de Seguridad
- Procedimiento de altas y bajas de usuarios
- Política de Uso aceptable de activos proporcionados
- Política de Mesas Limpias
- Política de Control de Accesos
- Política de Copias de Seguridad
- Política de intercambio de información con terceros
- Política de adquisición y mantenimiento de sistemas IT y desarrollo seguro
- Política de Gestión de Incidentes de Seguridad
- Política General de Continuidad de Negocio
- Política de gestión de proveedores

2. Alcance

Esta política de seguridad de la Información y los procedimientos relacionados serán de aplicación para todos los departamentos de Madiva y todas las sociedades del grupo.

En adelante, cualquier referencia a Madiva se entenderá referida a Madiva.

3. Audiencia

Todo el personal de Madiva tiene que conocer y cumplir obligatoriamente esta política, particularmente aquellos con responsabilidades en tecnología o en gestión de Información, así como el Responsable de Seguridad de la Información (CISO a partir de ahora).

4. Excepciones y correcciones a la política

Excepciones, modificaciones y comentarios a la presente política se realizarán siguiendo el procedimiento de “Gestión de excepciones a las políticas corporativas”.

5. Controles organizativos

5.1 Políticas para la seguridad de la información

La Política de Seguridad de la Información de Madiva establece los requisitos concisos y mínimos a cumplir por todos los departamentos de la empresa.

El responsable de la Política de Seguridad de la Información es el CISO de Madiva y debe ser aprobada por el Comité SGSI.

Los procedimientos y políticas relativos a los que se haga referencia en la Política de Seguridad de la Información serán asimismo responsabilidad del CISO de la compañía y para su modificación será necesario, como mínimo, la aprobación por parte de los siguientes roles:

- CISO
- Director de IT
- Responsable de Cumplimiento

La política de Seguridad de la Información y las políticas y procedimientos asociados de Madiva estarán disponibles para todos los trabajadores de la empresa en la intranet corporativa.

El CISO se debe encargar de liderar la revisión de la Política de Seguridad de la Información anualmente, así como de las políticas y procedimientos relacionados.

5.2 Funciones y responsabilidades en materia de seguridad de la información

A continuación, se describen los roles implicados en la gestión de la Seguridad de la Información y sus responsabilidades:

- **Consejero delegado (CEO)**
    - Es informado de la política de la Seguridad de la Información y es el responsable de proveer el liderazgo y la estructura de gestión necesaria, así como los recursos necesarios, para la implementación de la Política de Seguridad de la Información.

- Se asegura de la integración de los requisitos de Seguridad de la Información en todos los procesos de negocio.
- Participa en la revisión de las políticas y actividades de Seguridad de la Información.
- Es informado de la implementación de la Política de la Seguridad en los diferentes departamentos, incluyendo el cumplimiento legal y normativo.
- Es responsable de la aprobación de la financiación de las actividades de Seguridad de la Información.

- **Responsable de Seguridad de la Información (CISO)**
  - Asegurar que la Política de Seguridad de la Información esté alineada con la actividad de la empresa.
  - Se le informa de todas las actividades del negocio relacionadas con Seguridad de la Información.
  - Comunica e interactúa regularmente con empleados y la dirección acerca de los procesos y actividades definidos en la política de Seguridad de la Información.
  - Da soporte al negocio en la implementación y ejecución de la Política de Seguridad de la Información y sus procesos relacionados.
  - Colabora en la creación y mantenimiento de la información relativa a los Riesgos de Seguridad de la compañía.
  - Participa en el ciclo de vida de los proyectos tecnológicos cuando es necesario o requerido.
  - Es responsable de la evaluación de Seguridad de los proveedores externos siguiendo las directrices de Madiva definidas en la Política de Seguridad de la Información.
  - Es el responsable de la creación y comunicación a la compañía de las tareas de concienciación en Seguridad, así como de preparar el material necesario referente a los nuevos empleados.
  - Debe estar informado de las tendencias de la industria. Por ejemplo, asistiendo a conferencias, cursos o grupos de trabajo y/o fórums con la Seguridad de la Información.
  - Es el responsable de analizar los incidentes de seguridad y liderar el plan de Respuesta a Incidentes en caso de ser necesario.

- **Delegado de protección de datos**
  - Informar y asesorar al responsable o al encargado del tratamiento y a los empleados de las obligaciones que les incumben en todo lo relacionado con la implantación de políticas de Protección de Datos.
  - Comprobar el cumplimiento del RGPD, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes
  - Ofrecer el asesoramiento relativo a las evaluaciones de impacto y la supervisión del cumplimiento normativo de su aplicación interna.
  - Asesorar a los empleados durante el tratamiento de datos.
  - Supervisar el adecuado cumplimiento de las normas sobre protección de datos en la entidad.

- Revisar las políticas internas de privacidad en la organización y su adecuación normativa.
- Asignar responsabilidades entre los miembros de la organización, respecto a las obligaciones en materia de protección de datos.
- Realización de acciones de concienciación internas respecto al cumplimiento efectivo de la normativa.

- **Responsable de la Información**
  - Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
  - Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
  - Tiene la potestad de determinar los niveles de seguridad de la información.

- **Responsable del servicio**
  - Es el responsable de determinar los niveles de seguridad de los servicios.

- **Responsable del sistema**
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

- **Administrador de seguridad**
  - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
  - La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
  - La aplicación de los Procedimientos Operativos de Seguridad (POS).
  - Asegurar que los controles de seguridad establecidos son adecuadamente observados.
  - Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.3 Segregación de tareas

Se deben implementar controles para asegurar que una persona no pueda realizar las siguientes funciones simultáneamente:

- Gestión de usuarios (añadir, modificar o borrar usuarios o permisos y autorizaciones, así como cambio de contraseñas) y aprobación de cambios en los usuarios.
- Revisión auditoría de la seguridad y sus registros e Implementación/operación de los controles de seguridad.

El Responsable de cumplimiento velará por asegurar el correcto cumplimiento de los controles de segregación de tareas.

5.4 Responsabilidades de la dirección

Es responsabilidad de la Dirección que el personal:

- Esté debidamente informado de sus funciones y responsabilidades en materia de seguridad de la información antes de que se le conceda acceso a la información de la organización y a otros activos asociados.
- Dispongan de directrices que establezcan las expectativas en materia de seguridad de la información de su función dentro de la organización.
- Cumplan con la política de seguridad de la información y las políticas y procedimientos asociados.
- Alcancen un nivel de concienciación sobre la seguridad de la información pertinente para sus funciones y responsabilidades dentro de la organización.
- Cumplan con los términos y condiciones de empleo.
- Mantener las competencias y cualificaciones adecuadas en materia de seguridad de la información mediante una formación profesional continua.
- Dispongan de un canal confidencial para denunciar infracciones de la seguridad de la información, políticas o procedimientos específicos de seguridad de la información.
- Dispongan de los recursos adecuados y del tiempo necesario para planificar la aplicación de los procesos y controles de seguridad de la organización.

5.5 Contacto con las autoridades

El CEO será el encargado de contactar con las autoridades en lo referente a incidentes de Seguridad de la Información, salvo con las autoridades en materia de Protección de Datos, con las que se comunicará el Delegado de Protección de datos.

5.6 Contacto con grupos de interés especial

El CISO mantendrá contactos y/o participará en grupos de especial interés, así como en foros especializados en seguridad de la Información con los objetivos de compartir información sobre actividades fraudulentas, mejorar el conocimiento de las mejores prácticas en materia de Seguridad de la Información, mantenerse al día de las tendencias en tecnologías de seguridad y en tecnologías o métodos utilizados en el mercado para vulnerar la seguridad de las empresas, mantener contacto con especialistas en seguridad, y conocer el estado del arte de las principales vulnerabilidades y amenazas existentes en el sector.
Las peticiones de información por parte de interesados referentes a Seguridad de la Información serán gestionadas en coordinación con el CISO.

5.7 Inteligencia sobre amenazas

Para identificar y evaluar las amenazas a la seguridad de la información que puedan aparecer, Madiva se ha subscrito a las siguientes listas de distribución de informes y noticias de seguridad:

- INCIBE: https://www.incibe.es/incibe-cert/simplenews/subscriptions/landing
- US-CERT: https://www.cisa.gov/about/contact-us/subscribe-updates-cisa
- CIS RSS: https://www.cisecurity.org/rss-syndication/
- MSRC: https://blogs.technet.microsoft.com/msrc/

5.8 Seguridad de la información en la gestión de proyectos

En cada nuevo proyecto que implique cambios tecnológicos a implementar por la empresa se incluirá un proceso de revisión por parte del CISO para asegurar el correcto cumplimiento de la presente Política de Seguridad de la Información.

Todos los procesos de revisión que afecten a la gestión de la información de la compañía serán documentados en el proyecto en base a las recomendaciones del CISO.

Los proyectos que impliquen tratamientos de datos personales deberán ser informados asimismo al departamento de protección de datos.

5.9 Inventario de la información y otros activos asociados

Se deben identificar los activos asociados con la información y los sistemas que la tratan y se debe hacer y mantener un inventario de esos activos. Se entiende como activo todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, medios magnéticos etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Se han de identificar los activos relevantes durante todo el ciclo de vida de la información de Madiva (creación, proceso, almacenado, transmisión, borrado y destrucción) y documentarlos. Este inventario se ha de mantener actualizado y para cada activo identificado se ha de identificar el propietario y el tipo de información que trata.

Todas las áreas son responsables de asegurarse que se mantiene un inventario de activos utilizados en su departamento o por externos contratados por su departamento informando a IT/CISO de cualquier nueva instalación de HW o SW. El departamento de IT será el encargado de mantener dicho inventario y realizar revisiones anuales con los departamentos.

Para cada activo se debe definir como mínimo:

- Propietario
- Identificador
- Clasificación de la información que trata (si gestiona o no datos sensibles y/o confidenciales).
- Descripción breve

5.10 Uso aceptable de la información y otros activos asociados

Con la finalidad de evitar el uso de los recursos y dispositivos de tratamiento de información para fines no autorizadas o ajenas al negocio se han fijado directrices de seguridad aplicables a todos los usuarios de los sistemas de información de Madiva, alineada con la Política de Seguridad de la Información.

Por tanto, Madiva pone a disposición de sus trabajadores y colaboradores los más robustos sistemas tecnológicos que contribuyan a una mayor operatividad y eficiencia para preservar la integridad de estos sistemas y dispositivos, evitar pérdidas de datos y/o un uso ilícito o no autorizado.

Los activos de información, inventariados, clasificados y etiquetados deben contar con medidas oportunas para asegurar la disponibilidad segura de las mismas a los usuarios debidamente autorizados quienes asumen la responsabilidad de su manipulación.

Procedimiento de manipulación:

Las acciones dependen de la clasificación de la información y su posición en el ciclo de vida del activo.

- Cualquier nuevo activo de información se creará como de “Uso Interno” por defecto, y el propietario mantendrá o cambiará este nivel de clasificación acorde con la información incluida.
- La Información no clasificada se considerará como “Pública”.
- Se registrará la cadena de custodia de cualquier evento de seguridad relevante.
- Los acuerdos con prestadores de servicio que conlleven intercambio de información tendrán en consideración el ámbito de aplicación del presente documento y sus propios procedimientos para lo que les sea aplicable.

5.11 Devolución de los activos

- Todos los empleados y usuarios externos deben devolver todos los activos de Madiva que estén en su poder al terminar su empleo, contrato o acuerdo.
- El proceso de finalización de contrato y acuerdo debe formalizarse para incluir la devolución de todos los documentos físicos y activos electrónicos propiedad de Madiva o confiados a ella.

- En los casos en que un empleado o un usuario externo adquiere el equipo de la organización o utiliza su propio equipo personal, se deben seguir procedimientos para asegurar que toda la información pertinente sea transferida a la organización y borrada de forma segura del equipo.
- Durante el período de notificación de finalización de contrato o empleo, se controlará la copia no autorizada de información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados y proveedores implicados.

5.12 Clasificación de la información

Los propietarios de la Información deben clasificar la información bajo su control en una de las siguientes categorías:

- CONFIDENCIAL
- INTERNA
- PÚBLICA

Toda la información por defecto será considerada INTERNA, a no ser que se considere explícitamente lo contrario.

Los datos personales considerados en categorías especiales según las leyes españolas de protección de datos serán considerados con la categoría Confidencial.

Toda la información clasificada como Confidencial tendrá que almacenarse de manera cifrada y el acceso a la misma se realizará siempre mediante canales cifrados.

Madiva podrá establecer procedimientos especiales para el tratamiento de la información confidencial.

5.13 Etiquetado de la información

Los activos de información inventariados y clasificados deben ser etiquetados para permitir la identificación de la información en ellos contenidos, siendo necesaria la concienciación de los usuarios para asegurar la confidencialidad y seguridad de estos.

La responsabilidad del etiquetado recaerá sobre los propietarios, el Responsable del SGSI y/o bien sobre los usuarios finales, debiendo seguirse el procedimiento oportuno.

El etiquetado, en todo caso, debe tener carácter restringido no pudiendo visualizarse externamente, para evitar de esta forma la identificación de información sensible o crítica por personas no autorizadas para su visualización o acceso.

Los documentos que contengan información clasificada como confidencial deben ser correctamente identificados como tal, incluyendo correos electrónicos.

5.14 Transferencia de información

El intercambio de información puede producirse a través de diferentes tipos de dispositivos de comunicación incluyendo correo electrónico, voz, vídeo, etc.

El intercambio de software puede producirse a través de diferentes medios, incluyendo descargas desde Internet, así como la compra a proveedores de productos comerciales.

Las operaciones de negocio de la Organización pueden ser interrumpidas y la información verse comprometida si los dispositivos de comunicación fallan, se sobrecargan o interrumpen. La información puede verse comprometida si es accesible a usuarios no autorizados.

Corresponde identificar los mecanismos especiales para proteger los activos críticos al Responsable de Seguridad de la Información, validando los intercambios de información y software entre Madiva y terceras organizaciones.

El intercambio de información o software clasificados como de uso interno, restringido o confidencial que se realice con otras organizaciones, debe estar formalizado en acuerdos, que deben establecer las condiciones en las que se realizarán dichos intercambios.

Cuando, por razones de urgencia y eficiencia del servicio, sea imposible la formalización previa de dicho acuerdo, el intercambio de información estará sujeta a las condiciones generales previstas en este procedimiento y será el remitente el responsable de su cumplimiento.

El intercambio debe realizarse respetando la clasificación y el etiquetado de la información que se maneje durante dicho intercambio, de acuerdo con lo especificado en el procedimiento pertinente.

Los intercambios de información clasificada como restringida, así como de datos de carácter personal de alto nivel, se deben realizar empleando mecanismos de cifrado que impidan la divulgación no autorizada de acuerdo con lo establecido en el apartado de “criptografía”.

Es necesario establecer acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección. Estos acuerdos deberían tratar puntos tales como:

- La responsabilidad de las partes en el uso y protección y custodia de la información.
- La trazabilidad de los datos.
- El cumplimiento de las normas técnicas y legales.
- Los requisitos de cifrado.
- Las responsabilidades en la cadena de custodia.
- Los controles de acceso a la información.

En los acuerdos se deben establecer los mecanismos oportunos para facilitar la gestión de estos intercambios y plasmar las responsabilidades y obligaciones legales cuando se lleven a cabo, especialmente las relacionadas con los datos de carácter personal.

Estos acuerdos deben indicar las responsabilidades de control y notificación del envío, transmisión y recepción de la información que se intercambia. Se debe asignar un gestor para cada acuerdo con la responsabilidad de controlar y hacer un seguimiento de su desarrollo.

En el ámbito legal, los acuerdos deben establecer las responsabilidades y obligaciones legales relativas al intercambio, especialmente aquellas derivadas del intercambio de datos de carácter personal con otras entidades, cesionarias o cedentes, de acuerdo con la legislación vigente sobre protección de datos de carácter personal.

No se podrán realizar intercambios de aquella información clasificada como confidencial.

El correo electrónico debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, integridad y disponibilidad de la información.

El servicio de correo tiene por finalidad permitir la comunicación electrónica entre los trabajadores. Es por ello por lo que deben garantizarse unos requerimientos mínimos de disponibilidad del servicio, así como de confidencialidad, integridad y autenticidad de los mensajes de correo, para la consecución de los objetivos de negocio de Madiva.

Los servidores de correo deben encontrarse actualizados en lo referente a parches de seguridad, contar con una correcta gestión de accesos y disponer de mecanismos de protección frente a posibles infecciones por virus y recepción de correo basura o spam.

5.15 Control de acceso

La "Política de control de accesos" recoge las condiciones en las que se permite el acceso a la oficina, incluyendo accesos temporales, así como las condiciones de acceso a los recursos lógicos y físicos (activos) de Madiva.

5.16 Gestión de identidades

Para acceder a cualquier plataforma o servicio de Madiva será necesario el uso obligatorio de credenciales de accesos asignadas a personas nominales y documentadas.

Corresponde, por un lado, a la Dirección realizar la solicitud de alta y baja en los sistemas de información de usuarios internos, y por otro, a los responsables de cada sistema informar de la necesidad de autorizar el acceso de cada uno de sus usuarios internos y externos.

La asignación de identificadores de usuario se realizará a través de un procedimiento formal de registro.

Además, se creará un registro lógico, con respaldo físico, de todos los usuarios existentes en el sistema, verificando que se indican: **datos personales, detalles de alta y de los accesos requeridos y detalle de la baja.**

Se realizará una verificación periódica de los usuarios obsoletos en el sistema, no utilizados, bloqueados, para su estudio y eliminación en caso de ser necesario.

Esta comprobación se realizará con una periodicidad no superior a los requerimientos de seguridad exigidos por la legislación en materia de protección de datos de carácter personal. Los resultados serán comunicados al propietario de los activos de información.

Cuando se conozca la baja de un empleado, la Dirección será la responsable de notificarlo al propietario de la información o a quien éste haya delegado, para su deshabilitación (baja) en los sistemas de información.

En el caso de la finalización de la relación contractual con un colaborador externo, el responsable pondrá en conocimiento del propietario de los datos o en quien éste haya delegado, para su baja en los sistemas de información.

5.17 Información de autenticación

Para la autentificación a cualquier sistema de información, todo usuario debe disponer de unas credenciales de carácter reservado (contraseña), identificador único aun cuando puedan utilizar diferentes formas de acreditarse en función del sistema de información.

Corresponderá al Responsable de los sistemas el reajuste de los privilegios de acceso, tras las revisiones realizadas por los responsables de cada área de negocio.

A través de herramientas previamente identificadas se asegurará que sólo usuarios autorizados tengan acceso a cuentas privilegiadas con el fin de reducir el riesgo de accesos no autorizados a los sistemas de información y para garantizar un funcionamiento correcto de los sistemas de autentificación.

Las credenciales asociadas a identificadores de usuarios que tengan asignados privilegios de administración deben cumplir requerimientos de calidad de contraseñas más estrictos que para el resto de los usuarios finales.

Una vez que las credenciales han sido generadas y verificadas, conforme a los requerimientos establecidos, se facilitarán a los usuarios a través de canales que mitiguen el riesgo de que sean interceptadas por terceros no autorizados para analizar, detectar y alertar de comportamiento anómalo de usuarios de cuentas privilegiadas, permitiendo una respuesta rápida por parte del equipo de incidentes.

Al igual que el identificador de usuario, la contraseña de acceso a los Sistemas se deberá considerar personal e intransferible, tendrá carácter secreto y no se permitirá la divulgación de la clave en ninguna circunstancia a otras personas integrantes de la plantilla o ajenas a la Organización, salvo imposibilidad operativa previamente autorizada.

Las contraseñas están clasificadas como información confidencial de acuerdo con el esquema de clasificación de la información de Madiva, por lo que cada usuario será responsable de mantener la confidencialidad de su contraseña y de cualquier trabajo realizado con ella.

Asimismo, corresponderá a los Responsables de Sistemas la autorización de almacenamiento de contraseñas en programas, scripts o códigos desarrollados para la conexión automática a los sistemas de información, y a la Dirección determinar el uso correcto de las contraseñas y comunicación si existiesen sospechas de uso indebido.

El carácter secreto de las contraseñas obliga a que no se divulguen de ninguna manera.

Cualquier sospecha de la pérdida de confidencialidad de una contraseña originará una solicitud de cambio de contraseña en el mínimo tiempo posible.

El usuario cooperará en el mantenimiento de la eficacia de la seguridad mediante la comunicación de cualquier sospecha de posible mal uso de las contraseñas.

5.18 Derechos de acceso

La creación de identificadores de usuario y provisión de accesos de este se realiza a través de un procedimiento formal (Instrucción de creación de identificadores de usuarios y provisión de accesos).

Los responsables de cada Sistema involucrado son los encargados de indicar las funciones que su usuario realizará en el sistema para asignarle un perfil de acceso que se ajuste a ellas. En caso de no existir tal perfil se procederá a crearlo.

En la medida de lo posible para la creación de los perfiles se deberá realizar las siguientes comprobaciones:

- Verificación que la autorización del usuario ha sido realizada por el responsable del área de negocio propietaria de los activos. Dicha autorización podrá ser implícita o explícita, según se determine en cada caso, y podrá estar delegada al efecto.

- Los responsables contarán con un registro de las personas con acceso a la información, de acuerdo con los requerimientos de seguridad exigidos por la legislación vigente en materia de protección de datos de carácter personal.
- Verificación de idoneidad del nivel de acceso en relación con los objetivos del negocio y las responsabilidades establecidas para cada perfil.
- Comprobar que cada usuario accede a los sistemas en los que realmente tiene permiso, y posee la autorización adecuada.
- En la creación de identificadores de usuario con un período de vigencia conocido o validez temporal, como por ejemplo de empleados con contratos temporales, empleados de las organizaciones subcontratadas, etc., y siempre que el sistema lo permita, se establecerá la fecha de expiración automática de validez del identificador. Consecuentemente, los administradores deberán activar los parámetros necesarios en los sistemas para que estos identificadores se bloqueen automáticamente cuando venza su período de vigencia.
- Adicionalmente, y de forma periódica, se realizará una revisión de los registros de acceso a los sistemas para todos los usuarios.

Revisión de derechos de acceso

El acceso a los recursos disponibles de cada área de negocio deberá gestionarse de manera adecuada, asignándose según la necesidad de los usuarios que emplean dichos recursos.

Bajo la supervisión del Responsable del SGSI se realizará, de forma periódica en la medida de lo posible, tareas de verificación de la concordancia entre la asignación de privilegios a usuarios, recogida en el inventario de usuarios, y las necesidades reales derivadas de la actividad que desarrollen. Para dichas revisiones podrá apoyarse en las áreas competentes que se definan a tal efecto.

Durante el proceso de revisión deberán comprobarse -en la medida de lo posible- los siguientes aspectos:

- Derechos de acceso asignados a todos los usuarios, con la periodicidad que se establezca en los procedimientos correspondientes y según las necesidades identificadas.
- Se comunicará al responsable de los activos de información correspondientes, los derechos de acceso de los usuarios para que comprueben si estos son correctos.

Adicionalmente a lo indicado con anterioridad, durante el proceso de revisión de los derechos de acceso de usuarios privilegiados deberán comprobarse los siguientes aspectos:

- Los derechos de acceso de los usuarios con privilegios especiales en los sistemas se revisarán con una periodicidad menor a la establecida para los usuarios finales.
- Asimismo, se monitorizarán las actividades de los usuarios con privilegios especiales en el sistema.

Se informará a la Dirección de aquellos hechos que hayan sido observados. Las irregularidades serán comunicadas, a los Responsables de los Sistemas, y a los Administradores, que procederán a su reajuste.

Retirada o reasignación de derechos de acceso

De igual forma que en la asignación de usuario, cuando se conozca la baja de un empleado, la Dirección será el responsable de notificar al propietario de la información o a quien éste haya delegado, para la retirada de sus derechos de acceso asociados a su identificador usuario.

En el caso de la finalización de la relación contractual con un colaborador externo, el Responsable del Sistema pondrá en conocimiento del propietario de los datos o en quien éste haya delegado para la retirada de sus derechos de acceso asociados a su identificador usuario.

Las modificaciones en los privilegios de un usuario derivadas de cambios organizativos serán competencia de los responsables de las áreas organizativas de origen y destino, en coordinación con el área de negocio implicada, con el propósito de garantizar que el usuario mantenga únicamente los privilegios que le correspondan para el ejercicio de sus funciones.

5.19 Seguridad de la información en las relaciones con los proveedores

Dentro de la "Política de gestión de proveedores" detallan los requisitos de evaluación en materia de seguridad de la información a los mismos.

5.20 Seguridad de la información en los acuerdos con los proveedores

Madiva ha establecido y mantiene un registro de acuerdos con partes externas (contratos o acuerdos de intercambio de información) para hacer seguimiento de a dónde va su información. Dichos acuerdos se revisan y actualizan periódicamente para asegurarse de que siguen siendo necesarios y de que se ajustan a las cláusulas de seguridad de la información pertinentes.

5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Se definen los requisitos de seguridad de la información que son responsabilidad de los proveedores de servicio y se evalúa los controles de seguridad adecuados.

5.22 Monitorización, revisión y gestión del cambio de los servicios de proveedores

Se establecen mecanismos de monitorización de los servicios proporcionados y manejados por los proveedores. A su vez, se supervisan los cambios en los servicios de los proveedores incluyendo los cambios y mejoras en las redes, el uso de nuevas tecnologías, cambios en la ubicación física de las instalaciones de servicios y subcontratación de otro proveedor.

5.23 Seguridad de la información para el uso de servicios en la nube

Madiva evalúa y gestiona los riesgos asociados con la adopción de servicios en la nube, asegurando la confidencialidad, integridad y disponibilidad de la información almacenada o procesada en estos entornos. A su vez, se establecen acuerdos contractuales claros con los proveedores de servicios en la nube para garantizar un uso seguro y conforme a la política de seguridad de la información.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Los incidentes de seguridad serán reportados al CISO, Delegado de Protección de datos y al responsable de servicios jurídicos, y se coordinarán para aplicar las actividades detalladas en la "Política de gestión de incidentes de seguridad de la información".

5.25 Evaluación y decisión sobre los eventos de seguridad de la información

Se detallará la evaluación y decisión sobre los eventos de seguridad dentro de la "Política de gestión de incidentes de seguridad de la información".

5.26 Respuesta a incidentes de seguridad de la información

Se ha detallado una "Política de Gestión de Incidentes de Seguridad" con el fin de controlar el proceso de resolución ante incidentes y la capacidad para resolverlo. Los incidentes deben de quedar correctamente registrados de la manera que se detalla en la política.

5.27 Aprender de los incidentes de seguridad de la información

Se debe de revisar y analizar los incidentes producidos como mínimo anualmente por parte del CISO. Para llevar a cabo dicho análisis los registros de los incidentes deben de estar correctamente almacenados y mantenidos bajo copias de seguridad.

5.28 Recopilación de evidencias

Las evidencias obtenidas sobre las incidencias registradas deben registrar un determinado conjunto de valores y acciones mínimas con el fin de facilitar la trazabilidad del incidente. La definición de las necesidades mínimas de registro se encuentra recogidas dentro de la "Política de gestión de incidentes de seguridad de la información".

5.29 Seguridad de la información durante la interrupción

Los aspectos de seguridad de la información durante la interrupción se detallan en la "Política General de continuidad de negocio".

5.30 Preparación para las TIC para la continuidad del negocio

Se debe garantizar la continuidad de las operaciones de la organización en caso de interrupciones en los servicios de nube y garantizar que los servicios críticos estén disponibles y sean recuperables en un período de tiempo razonable. Se ha desarrollado una "Política General de continuidad de negocio" que incluye estrategias específicas para garantizar la disponibilidad y recuperación de servicios críticos en caso de interrupciones.

5.31 Identificación de requisitos legales, reglamentarios y contractuales

Todos los requisitos legislativos, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y actualizados.

Los directivos o responsables identifican toda la legislación aplicable a sus organizaciones para cumplir con los requisitos de su tipo de negocio.

5.32 Derechos de propiedad intelectual (DPI)

Se establecerán procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de producción de software patentado.

Cualquier actividad relacionada con información o material sujetos a derechos de propiedad intelectual deberá tener en cuenta las restricciones legales a este respecto.

Específicamente, se deberán establecer acuerdos con fabricantes de productos del software o del material protegido (documentos, informes, material multimedia, etc.) para el cumplimiento de los derechos de autor. Adicionalmente, los usuarios deberán estar informados acerca de los derechos de propiedad intelectual, prohibiendo de manera explícita la copia de material protegido por los derechos de autor.

Deberán establecerse los responsables que lleven a cabo la gestión de las licencias de software, contactos con los proveedores de software, actualización de versiones y número de licencias.

Adicionalmente, se deberá establecer un inventario con todas las licencias vigentes de productos de software o material incluyendo al menos:

- Nombre del producto o material.
- Número de licencia.
- Periodo de validez de la licencia.
- Ubicación física donde se custodia la licencia.
- Número máximo de usuarios permitidos.
- Relación de máquinas en las que se encuentra instalado (si aplica).

Se deberán establecer todas las medidas necesarias para asegurar el cumplimiento de las limitaciones impuestas por los fabricantes de software o de material bajo licencia de los productos adquiridos.

En caso de incumplimiento de las políticas de protección de derechos de autor sobre determinado software o material protegido por algún usuario se tomarán las medidas disciplinarias oportunas.

Adicionalmente, se deben tener en cuenta las limitaciones técnicas o de coste que indiquen los responsables de informática; aunque la decisión última de la adquisición de software y, por lo tanto, de que se incluya en la lista de software autorizado será del responsable del área implicada que lo necesite para el desarrollo de las funciones encomendadas a la misma.

En definitiva, se deben tener en cuenta las siguientes directrices para proteger cualquier material que pueda ser considerado propiedad intelectual:

- Publicar las directrices para el cumplimiento de los derechos de propiedad intelectual que definan el uso legal de los productos software y de los de información.

- Adquirir software únicamente a través de las fuentes conocidas y de confianza para garantizar que no se infringen los derechos de autor.
- Mantener el conocimiento de las directrices de protección de los derechos de propiedad intelectual.
- Mantener registros adecuados de los activos e identificar todos los activos que requieran la protección de los derechos de propiedad intelectual.
- Mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.
- Implementar controles para garantizar que no se exceda el número máximo de usuarios permitidos por la licencia.
- Llevar a cabo comprobaciones de que sólo se instala software autorizado y productos licenciados.
- Disponer de un procedimiento para mantener las condiciones de las licencias en forma adecuada.
- Disponer de un procedimiento para eliminar el software o para transferirlo a un tercero cuando cese su uso.
- Cumplir las condiciones contractuales del software y de la información que se obtenga de redes públicas.
- No duplicar ni convertir a otro formato y no extraer de grabaciones comerciales (audio, vídeo) nada más que lo que permita la ley de derechos de autor.
- No copiar parcial o totalmente libros, artículos, informes u otros documentos salvo lo que permita la ley de derechos de autor.

5.33 Protección de los registros

Se establecerán procedimientos y controles que garanticen la protección y almacenado de los registros de información en base a los requerimientos legales y contractuales existentes.

5.34 Revisión independiente de la seguridad de la información

Se deberán realizar revisiones independientes de la gestión de la seguridad, y el correcto cumplimiento de la política de seguridad y los controles definidos, como máximo cada dos años. Aunque las revisiones pueden ser realizadas por personal de Madiva, tendrán que ser de departamentos que no sean ni CISO ni IT para garantizar la independencia. El resultado de las revisiones se deberá registrar y reportar a la dirección para la correcta implementación de los planes de mejora y resolución de deficiencias encontradas.

5.35 Cumplimiento de las políticas y normas de seguridad de la información

Anualmente el CISO liderará una revisión del correcto cumplimiento de los controles de la política de seguridad de la información y políticas asociadas, documentando los resultados y las medidas propuestas para la correcta resolución de las deficiencias encontradas si es el caso.

5.36 Documentación de procedimientos operacionales

Los procedimientos operacionales y documentados para las actividades del sistema, siempre que sea pertinente por su naturaleza, se tratan como documentos formales cuyos cambios son autorizados por la Dirección.

Asimismo, de manera general, los sistemas de información se gestionan de manera sistemática, utilizando procedimientos equivalentes, similares y/o iguales (según corresponda), herramientas y recursos asignados de forma similar de acuerdo con las políticas y requerimientos.

En este sentido, los procedimientos operacionales especificarán -en la medida de lo posible- las instrucciones para la ejecución detallada de cada puesto de trabajo, incluyendo:

- Tratamiento y manipulación de la información.
- Copias de respaldo.
- Requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos más tempranos de comienzo y más tardíos de finalización posibles de cada tarea.
- Las instrucciones para manejar errores y otras condiciones excepcionales que puedan ocurrir durante la ejecución del trabajo, incluyendo restricciones en el uso de las utilidades del sistema.
- Los contactos del Soporte para el caso de dificultades operacionales o técnicas inesperadas.
- Las instrucciones para el manejo de resultados especiales y soportes, como el uso de papel especial o como la gestión de resultados confidenciales, incluyendo procedimientos de destrucción segura de resultados producidos como consecuencia de tareas fallidas.
- El reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema.
- La gestión de pistas de auditoría y de la información del registro de sistemas.

6. Controles de personas

6.1 Comprobación

Madiva dispone de un procedimiento de revisión de los posibles candidatos antes de la incorporación a la empresa en el que se definen las comprobaciones a realizar y el proceso a seguir. Este procedimiento es responsabilidad del departamento “Recursos Humanos” y ejecutado por el mismo.

6.2 Términos y condiciones de contratación

A todos los nuevos empleados se les proporcionará información referente a las Políticas de Seguridad de la Información de Madiva y sus responsabilidades.

También se les informará que los recursos proporcionados para su trabajo son propiedad de la empresa y se implementarán medidas de control y monitorización del uso de estos, y la totalidad de trabajadores firmarán un contrato de confidencialidad.

6.3 Concienciación, educación y formación en seguridad de la información

El CISO será el responsable de que, anualmente al menos, sea distribuida información sobre concienciación en Seguridad en Madiva a todos los trabajadores con acceso a los datos.

El departamento de Recursos Humanos será el responsable de que, en un plazo máximo a 30 días de su incorporación, a cada nuevo trabajador se le proporcione formación en materia de concienciación en Seguridad de la Información y cumplimiento con las leyes de Protección de Datos en vigor.

El CISO establecerá protocolos de “Mesas Limpias” en la que se incluirá la obligatoriedad del uso de contraseñas y bloqueo automático de los dispositivos con acceso a datos, así como el apagado responsable por parte de los usuarios al finalizar su jornada o excepcionalmente una vez a la semana. Este procedimiento es responsabilidad del CISO. Dichos protocolos estarán definidos en “Política de Mesas Limpias”. Además, se deberán guardar en cajones cerrados con llave todos los documentos que sean confidenciales o contengan datos personales.

6.4 Proceso disciplinario

El proceso disciplinario es el basado en el convenio (relativo al puesto de trabajo) cuyo responsable será el departamento de Recursos Humanos.

6.5 Responsabilidades ante la finalización o cambio

En la finalización del empleo o cambio en el puesto de trabajo, se debe tener en cuenta la seguridad para proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo, prestando especial atención:

- Comunicación de finalización del puesto de trabajo.
- Devolución de activos.

6.6 Acuerdos de confidencialidad o no divulgación

Los acuerdos de confidencialidad y no revelación protegen la información de la Organización e informan a los firmantes del acuerdo de sus responsabilidades relativas a la protección, utilización y revelación de información de una manera responsable y autorizada.

Dentro de una misma Organización, puede ser necesario utilizar diferentes formas de acuerdos de confidencialidad o no revelación para diferentes circunstancias.

Los acuerdos de confidencialidad y no revelación deberían cumplir con la legislación y reglamentación aplicable en la jurisdicción donde aplican.

Los requisitos de los acuerdos de confidencialidad y no revelación deberían revisarse periódicamente y siempre que se produzcan cambios que tengan influencia en dichos requisitos.

6.7 Teletrabajo

El teletrabajador debe mantener la máxima confidencialidad y discreción sobre el uso de información, datos y sistemas que están a su disposición como consecuencia del desarrollo de su actividad laboral fuera de las dependencias de Madiva. Este deber aplica tanto a información y datos de la propia compañía como de empresas clientes y proveedores. En el caso de que se maneje información en formato papel en el domicilio, debe custodiarse en lugar seguro y bajo llave o, en su defecto, protegida adecuadamente. En este sentido, también se extiende la aplicación de todo lo indicado en la Política de Seguridad de la Información.

- Todos los ordenadores portátiles y dispositivos móviles que tengan acceso remoto a datos clasificados como confidenciales deberán disponer de tecnología de encriptación de los datos tanto en la transmisión como en el almacenado.
- Las credenciales de acceso remoto creadas tendrán siempre caducidad, y nunca superior a 90 días.
- Se revisará y documentará periódicamente (periodicidad menor de 1 año) por parte del CISO los accesos externos otorgados y el uso de estos.

6.8 Notificación de los eventos de seguridad de la información

Los eventos de seguridad de la información incluyen, pero no se limitan a, intentos de acceso no autorizado, intrusiones, malware, pérdida o robo de dispositivos, fallos de seguridad, violaciones de políticas de seguridad, y cualquier otro incidente que pueda comprometer la seguridad de la información.

Todos los empleados y partes relacionadas deben reportar cualquier evento de seguridad que observen o del cual tengan conocimiento a través del canal de reporte designado

El reporte debe incluir información detallada sobre el evento, incluyendo fecha, hora, ubicación, descripción de lo ocurrido y cualquier evidencia relevante.

El equipo de seguridad de la información es responsable de evaluar y clasificar cada evento reportado en función de su gravedad y riesgo potencial.

Las debilidades de seguridad identificadas durante la evaluación de eventos o revisiones de seguridad deben ser documentadas y abordadas de manera oportuna

De esta forma, el trabajador Madiva tendrá la obligación de reportar a su superior más inmediato el evento o debilidad identificada para que salten los mecanismos definidos para mitigarlos.