CEU | Universidad San Pablo

CIBERSEGURIDAD

Actividad 1: Auditoría de un SGSI

Descripción breve

En esta actividad se busca aprender a trabajar con una herramienta de apoyo para realizar una auditoría del nivel de cumplimiento de gestión de la seguridad de una compañía.

Rafael María Urrios Álvarez Gómez

28 DE SEPTIEMBRE DE 2024

Contenido

1. Introducción

La auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo evaluar y garantizar la protección de la información dentro de Mapfre S.A., empresa multinacional que opera en más de 25 países y en diversas áreas de negocio, es fundamental implementar un SGSI robusto para proteger la confidencialidad, integridad y disponibilidad de su información. Este proceso de auditoría se realiza en conformidad con la norma ISO 27001. Este informe se centra en evaluar la conformidad de Mapfre S.A. con los requisitos de la norma ISO 27001, abarcando aspectos críticos de seguridad como la protección de la infraestructura tecnológica, la gestión de accesos privilegiados y la protección del código fuente. El propósito es identificar oportunidades de mejora y asegurar la continuidad y resiliencia del negocio frente a amenazas externas e internas.

2. Estándares base

Para la auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) de Mapfre S.A., se ha utilizado la norma ISO/IEC 27001 como referencia. Se seleccionaron 15 activos de vital importancia para la compañía y se implementaron 5 controles de seguridad en cada uno de los siguientes ámbitos: organización, personas, físicos y tecnológicos. Estos controles garantizan la protección integral de los activos críticos, alineándose con las mejores prácticas establecidas por la norma para asegurar la seguridad y confidencialidad de la información.

3. Descripción de la empresa

MAPFRE S.A. es una compañia multinacional española que opera en el sector asegurador y reasegurador, con presencia en 25 países y más de 38,000 empleados. Fundada en 1933, MAPFRE ofrece una amplia gama de productos y servicios aseguradores, financieros y de inversión, atendiendo tanto a particulares como a empresas. Su misión es proporcionar seguridad y protección a sus clientes, generando valor sostenible para sus accionistas, empleados y la sociedad en general. La empresa se guía por valores como la solvencia, la integridad, la innovación y la orientación al cliente, buscando siempre la excelencia en el servicio. Los seguros desempeñan un papel crucial en la sociedad al ofrecer protección financiera frente a riesgos e imprevistos, promoviendo la estabilidad económica y social. MAPFRE se compromete a ser un referente global en la industria aseguradora, contribuyendo al bienestar de sus clientes y al desarrollo sostenible de las comunidades donde opera.

4. Descripción del proyecto

El proyecto tiene como objetivo realizar una auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) en Mapfre S.A., en conformidad con la norma ISO 27001. Se han seleccionado 15 activos de vital importancia, que incluyen: el Router de conexión principal, el UPS principal del Data Center, la Red LAN de oficina central, los Backups diarios de sistemas críticos, el PC del Departamento Financiero, la Sala de servidores, los Discos duros externos de respaldo, el Equipo de Administradores de Sistemas, el Software de Gestión de Pólizas, el Servicio de correo electrónico corporativo, la Clave de cifrado de archivos confidenciales, el Sistema de climatización del Data Center, la Red WiFi corporativa, los Documentos en papel de pólizas y el Servidor de archivos compartidos. Para cada activo se especificará su tipo, subtipo, propietario, responsable, valor estratégico y una breve descripción. Además, se

llevarán a cabo un total de 20 controles de seguridad, distribuidos en 4 ámbitos: organización, personas, físicos y tecnológicos.

5. Categorización de activos

1) Activo 1: Router de conexión principal

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Arquitectura del sistema	Router de conexión principal	Departamento de infraestructura	Administrador de redes	0.00€	Muy Alto	Router que interconecta las redes internas con la ...

El Router de conexión principal es un componente crítico dentro de la arquitectura del sistema de Mapfre, operando como el punto de interconexión entre las redes internas y externas de la compañía. Propietario del Departamento de Infraestructura, este dispositivo, cuyo responsable es el Administrador de Redes, tiene un valor estratégico muy alto. Su función principal es garantizar la conectividad y seguridad en la transmisión de datos, permitiendo a Mapfre ofrecer servicios de seguros a sus clientes de manera eficiente y confiable.

2) Activo 2: UPS principal del Data Center

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Equipamiento auxiliar	UPS principal del Data Center	Departamento de TI	Tecnico de infraestructura	--	Alto	Sistema que proporciona energía de respaldo para e...

El UPS principal del Data Center es un sistema de alimentación interrumpida que proporciona energía de respaldo, evitando interrupciones en los servicios críticos de Mapfre. Este activo, gestionado por el Departamento de TI y con un responsable que es el Técnico de Infraestructura, tiene un valor estratégico alto. Su importancia radica en garantizar la continuidad del negocio, especialmente en situaciones de corte de energía, lo que permite a Mapfre mantener la disponibilidad de sus servicios en más de 25 países.

3) Activo 3: Red LAN de oficina central

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Redes de comunicaciones	Red LAN de oficina central	Departamento de TI	Administrador de redes	0.00€	Muy Alto	Red local que conecta todos los equipos dentro de ...

La Red LAN de oficina central es la red local que conecta todos los equipos dentro de la oficina principal de Mapfre. Este activo, de valor estratégico muy alto, es propiedad del Departamento de TI y es administrado por el Administrador de Redes. La red permite la comunicación y colaboración eficiente entre los empleados, facilitando la gestión de pólizas y la atención al cliente, pilares fundamentales de la operativa de Mapfre.

4) Activo 4: Backups diarios de sistemas críticos

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Datos / Información	Backups diarios de sistemas críticos	Departamento de Seguridad de la Información	Administrador de BBDD	--	Muy Alto	Copias de seguridad realizadas diariamente de los ...

Los backups diarios de sistemas críticos son copias de seguridad fundamentales para la protección de datos en Mapfre. Este activo, propiedad del Departamento de Seguridad de la Información y gestionado por el Administrador de Bases de Datos, tiene un valor estratégico muy alto. Estas copias se realizan diariamente para asegurar la recuperación de información vital, garantizando así la integridad de los datos y la continuidad de los servicios que ofrece Mapfre a sus clientes.

5) Activo 5: PC del Departamento Financiero

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Equipos informáticos (hardware)	PC del Departamento Financiero	Departamento Financiero	Administrador de Sistemas	--	Medio	Ordenador utilizado por el personal financiero par...

El PC del Departamento Financiero es un equipo informático utilizado por el personal financiero de Mapfre para llevar a cabo sus labores diarias. Este activo, cuyo propietario es el Departamento Financiero y responsable el Administrador de Sistemas, tiene un valor estratégico medio. La disponibilidad y seguridad de este equipo son esenciales para la gestión financiera de la compañía, permitiendo un control eficiente de los recursos económicos.

6) Activo 6: Sala de servidores

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Instalaciones	Sala de servidores	Departamento de infraestructura	Técnico de infraestructura	--	Alto	Espacio físico destinado al alojamiento de servido...

La Sala de servidores es un recinto físico destinado al alojamiento de servidores y equipos críticos para las operaciones de Mapfre. Este activo es propiedad del Departamento de Infraestructura y gestionado por el Técnico de Infraestructura, teniendo un valor estratégico alto. La seguridad y control de acceso a esta sala son fundamentales para proteger la información sensible y garantizar la operativa continua de la empresa.

7) Activo 7: Discos duros externos de respaldo

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Soportes de información	Discos duros externos de respaldo	Departamento de TI	Administrador de Sistemas	--	Medio	Dispositivos de almacenamiento externos para copia...

Los discos duros externos de respaldo son dispositivos de almacenamiento utilizados por Mapfre para realizar copias de seguridad de datos importantes. Propiedad del Departamento de TI y gestionados por el Administrador de Sistemas, estos activos tienen un valor estratégico medio. Su uso es crítico para la recuperación de datos en caso de pérdidas o daños, asegurando que la información de los clientes y operaciones esté siempre protegida.

8) Activo 8: Equipo de Administradores de Sistemas

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Personal	Equipo de Administradores de Sistemas	Departamento de TI	Jefe de TI	--	Muy Alto	Personal encargado de la administración y mantenim...

El Equipo de Administradores de Sistemas es un grupo de profesionales que gestionan y mantienen los sistemas de TI de Mapfre. Este activo, de valor estratégico muy alto, es propiedad del Departamento de TI y su responsable es el Jefe de TI. La experiencia y competencia de este equipo son cruciales para la implementación de políticas de seguridad y la eficiencia operativa en todos los niveles de la empresa.

9) Activo 9: Software de Gestión de Pólizas

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Aplicaciones (software)	Software de Gestión de Pólizas	Departamento de Desarrollo	Líder de Proyecto	--	Muy Alto	Aplicación desarrollada internamente para gestiona...

El Software de Gestión de Pólizas es una aplicación desarrollada internamente por Mapfre para gestionar las pólizas de sus clientes. Este activo, de valor estratégico muy alto, es propiedad del Departamento de Desarrollo y su responsable es el Líder de Proyecto. La funcionalidad de este software es fundamental para la administración eficiente de pólizas, permitiendo a Mapfre ofrecer un servicio personalizado y efectivo a sus asegurados.

10) Activo 10: Servicio de correo electrónico corporativo

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Servicios	Servicio de correo electrónico corporativo	Departamento de TI	Administrador de Sistemas	--	Alto	Plataforma de correo para la comunicación interna ...

El Servicio de correo electrónico corporativo de Mapfre es una plataforma esencial para la comunicación interna y externa de la empresa. Este activo, de valor estratégico alto, es propiedad del Departamento de TI y administrado por el Administrador de Sistemas. Este servicio permite a los empleados comunicarse de manera efectiva, facilitando la colaboración en proyectos y la atención al cliente.

11) Activo 11: Clave de cifrado de archivos confidenciales

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Claves criptográficas	Clave de cifrado de archivos confidenciales	Departamento de Seguridad de la Información	Administrador de Seguridad	--	Muy Alto	Clave utilizada para cifrar archivos confidenciale...

La Clave de cifrado de archivos confidenciales es un componente crítico para la protección de la información sensible de Mapfre. Este activo, cuyo propietario es el Departamento de Seguridad de la Información y responsable el Administrador de Seguridad, tiene un valor estratégico muy alto. Su uso garantiza que los datos confidenciales estén protegidos contra accesos no autorizados, asegurando la confidencialidad de la información de los clientes.

12) Activo 12: Sistema de climatización del Data Center

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Equipamiento auxiliar	Sistema de climatización del Data Center	Departamento de Infraestructura	Técnico de Infraestructura	--	Alto	Sistema de aire acondicionado que regula la temper...

El Sistema de climatización del Data Center es fundamental para el correcto funcionamiento de los servidores y equipos críticos de Mapfre. Este activo, de valor estratégico alto, es propiedad del Departamento de Infraestructura y gestionado por el Técnico de Infraestructura. La regulación adecuada de la temperatura y humedad es esencial para prevenir daños en el hardware y garantizar la continuidad de los servicios ofrecidos.

13) Activo 13: Red WiFi corporativa

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Redes de comunicaciones	Red WiFi corporativa	Departamento de TI	Administrador de Redes	--	Medio	Red inalámbrica para la conexión de dispositivos m...

La Red WiFi corporativa de Mapfre permite la conexión de dispositivos móviles de los empleados, facilitando la movilidad y el acceso a la información. Este activo, de valor estratégico medio, es propiedad del Departamento de TI y administrado por el Administrador de Redes. La seguridad de esta red es vital para proteger la información de la compañía y asegurar que el acceso a los datos se realice de forma controlada.

14) Activo 14: Documentos en papel de pólizas

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Soportes de información	Documentos en papel de pólizas	Departamento Legal	Responsable de Archivo	--	Medio	Documentación física de pólizas almacenada en arch...

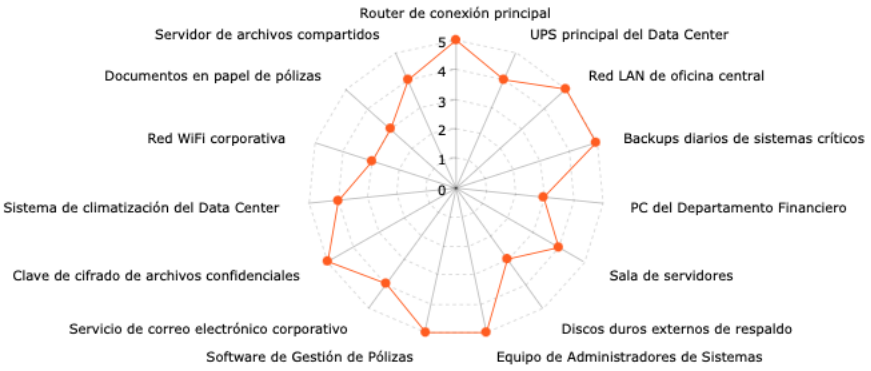
Los Documentos en papel de pólizas son la documentación física que respalda las pólizas emitidas por Mapfre. Este activo, propiedad del Departamento Legal y gestionado por el Responsable de Archivo, tiene un valor estratégico medio. La correcta gestión y almacenamiento de estos documentos son importantes para cumplir con las normativas legales y proporcionar un respaldo físico a los registros digitales.

15) Activo 15: Servidor de archivos compartidos

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Servicios	Servidor de archivos compartidos	Departamento de TI	Administrador de Sistemas	--	Alto	Servidor destinado a almacenar archivos de uso com...

El Servidor de archivos compartidos es un recurso utilizado para almacenar y compartir archivos entre los empleados de Mapfre. Este activo, de valor estratégico alto, es propiedad del Departamento de TI y administrado por el Administrador de Sistemas. Su funcionalidad permite la colaboración en proyectos y el acceso a documentos necesarios para el desempeño de las tareas diarias, contribuyendo a la eficiencia operativa de la empresa.

Mapa valor estratégico de los activo

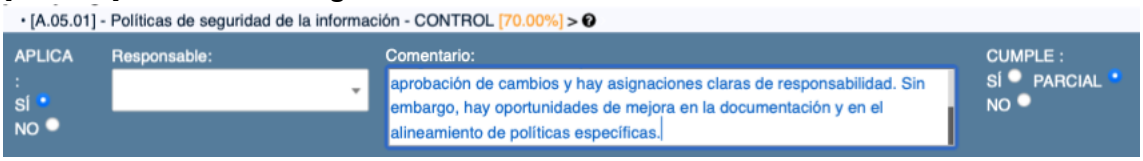


5 = Muy alto 0 = Muy bajo

6. Análisis de controles

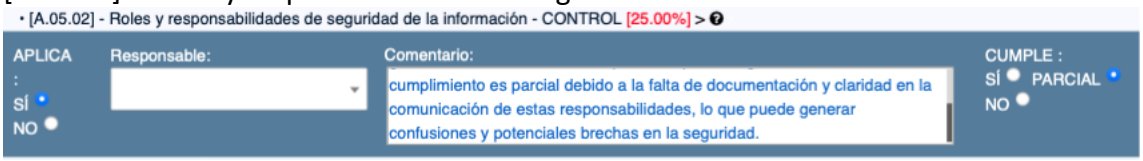
A) Organizativos

- [A.05.01] - Políticas de seguridad de la información



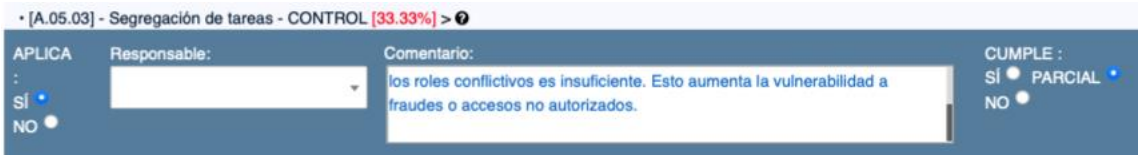
Mapfre cumple en gran medida con el control A.05.01, aunque presenta deficiencias en la implementación de políticas específicas y en la comunicación efectiva de las políticas al personal. Esto sugiere que, si bien hay un marco establecido, su aplicación y entendimiento pueden mejorarse para garantizar una seguridad de la información más robusta.

- [A.05.02] - Roles y responsabilidades de seguridad de la información



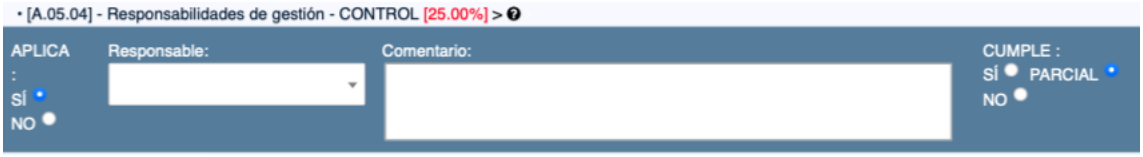
El control A.05.02 es fundamental para garantizar que las responsabilidades y roles de seguridad de la información estén claramente definidos y gestionados. En el caso de Mapfre, aunque la asignación de roles existe, su cumplimiento es parcial debido a la falta de documentación y claridad en la comunicación de estas responsabilidades, lo que puede generar confusiones y potenciales brechas en la seguridad.

- [A.05.03] - Segregación de tareas



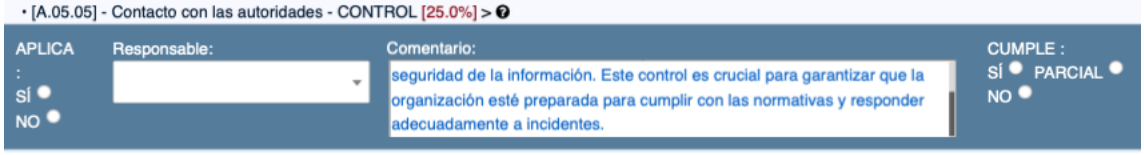
Mapfre cumple parcialmente con este control debido a la identificación de tareas que requieren segregación, pero no se han implementado completamente controles adecuados contra la colusión, y la supervisión de los roles conflictivos es insuficiente. Esto aumenta la vulnerabilidad a fraudes o accesos no autorizados.

- [A.05.04] - Responsabilidades de gestión



El control [A.05.04] presenta un marco para asegurar que la dirección está comprometida con la seguridad de la información, aunque Mapfre enfrenta áreas de mejora. A pesar de que hay políticas y procedimientos, la falta de una formación continua adecuada y la insuficiencia de canales confidenciales para la denuncia de violaciones limitan la efectividad del control. Esto expone a la organización a un riesgo medio alto, ya que la falta de concienciación puede llevar a incidentes de seguridad. Se recomienda que Mapfre implemente un programa de formación regular y establezca canales efectivos de denuncia para fortalecer su postura de seguridad.

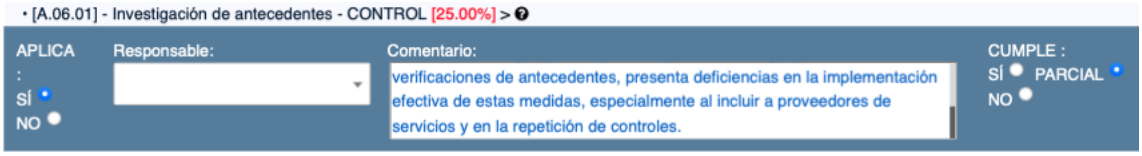
- [A.05.05] - Contacto con las autoridades



Mapfre cumple parcialmente con este control. Si bien hay procedimientos establecidos para contactar a las autoridades, no se especifican de manera clara las circunstancias y métodos de notificación. Esto puede limitar la efectividad de la respuesta ante incidentes y la comprensión de las expectativas de las autoridades.

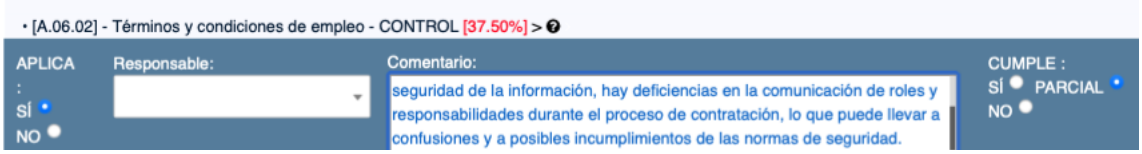
B) Personas

- [A.06.01] - Investigación de antecedentes



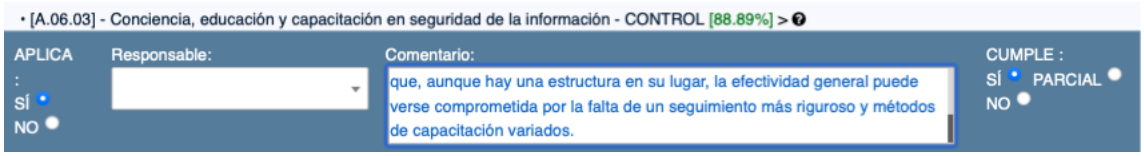
El control de investigación de antecedentes es esencial para asegurar que los empleados y colaboradores cumplan con los estándares de seguridad y confiabilidad requeridos por la organización. Mapfre cumple parcialmente con este control, ya que aunque tiene políticas en lugar para realizar verificaciones de antecedentes, presenta deficiencias en la implementación efectiva de estas medidas, especialmente al incluir a proveedores de servicios y en la repetición de controles.

- [A.06.02] - Términos y condiciones de empleo



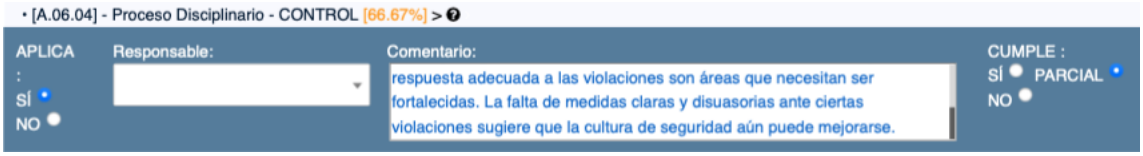
El control de Términos y Condiciones de Empleo en Mapfre muestra un cumplimiento parcial. Aunque se han implementado políticas que abordan la seguridad de la información, hay deficiencias en la comunicación de roles y responsabilidades durante el proceso de contratación, lo que puede llevar a confusiones y a posibles incumplimientos de las normas de seguridad.

- [A.06.03] - Conciencia, educación y capacitación en seguridad de la información



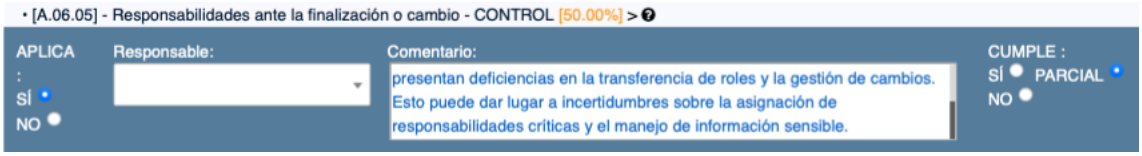
Mapfre ha tomado medidas para establecer un programa de concienciación y capacitación en seguridad de la información que sigue las políticas y procedimientos relevantes. Sin embargo, la implementación podría no ser totalmente efectiva en algunos aspectos, como la evaluación de la comprensión del personal y la variedad de métodos utilizados. Esto sugiere que, aunque hay una estructura en su lugar, la efectividad general puede verse comprometida por la falta de un seguimiento más riguroso y métodos de capacitación variados.

- [A.06.04] - Proceso Disciplinario



El control [A.06.04] sobre el Proceso Disciplinario es crucial para garantizar que se sigan procedimientos adecuados cuando hay infracciones a la política de seguridad de la información. Aunque Mapfre ha establecido un marco para gestionar las infracciones, la implementación efectiva y la respuesta adecuada a las violaciones son áreas que necesitan ser fortalecidas. La falta de medidas claras y disuasorias ante ciertas violaciones sugiere que la cultura de seguridad aún puede mejorarse.

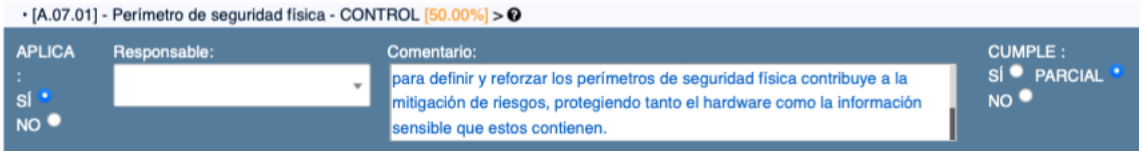
- [A.06.05] - Responsabilidades ante la finalización o cambio



El control sobre las responsabilidades ante la finalización o cambio de empleo en Mapfre se aplica en parte, ya que existen definiciones de responsabilidades que se mantienen tras la finalización del empleo, pero se presentan deficiencias en la transferencia de roles y la gestión de cambios. Esto puede dar lugar a incertidumbres sobre la asignación de responsabilidades críticas y el manejo de información sensible.

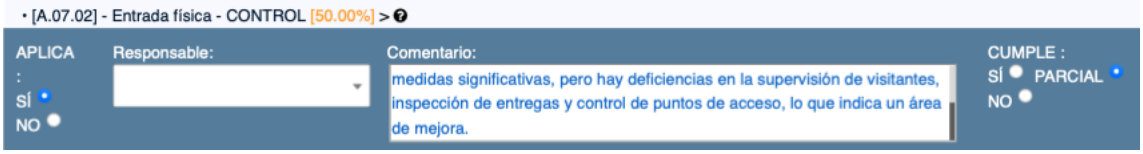
C) Infraestructuras

- [A.07.01] - Perímetro de seguridad física



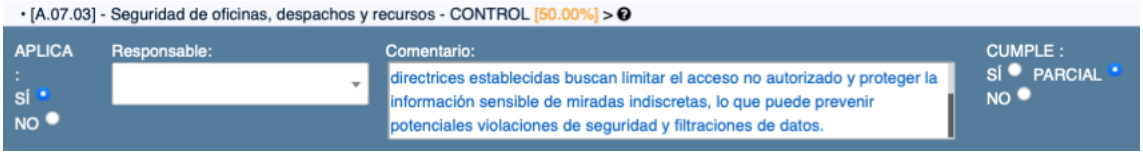
El control de perímetro de seguridad física es esencial para proteger los activos de información de una organización, asegurando que las instalaciones estén adecuadamente protegidas contra accesos no autorizados y amenazas externas. La implementación de directrices claras para definir y reforzar los perímetros de seguridad física contribuye a la mitigación de riesgos, protegiendo tanto el hardware como la información sensible que estos contienen.

- [A.07.02] - Entrada física



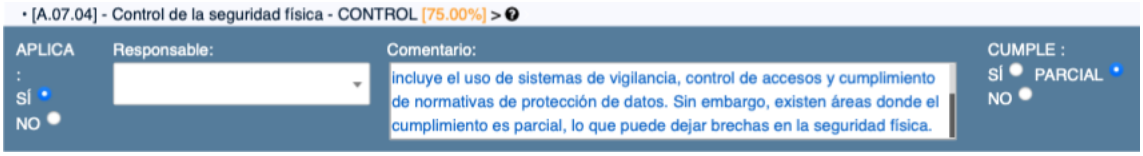
El control de entrada física es crucial para proteger la integridad y la confidencialidad de la información, así como para prevenir accesos no autorizados a instalaciones críticas. La organización ha implementado medidas significativas, pero hay deficiencias en la supervisión de visitantes, inspección de entregas y control de puntos de acceso, lo que indica un área de mejora.

- [A.07.03] - Seguridad de oficinas, despachos y recursos



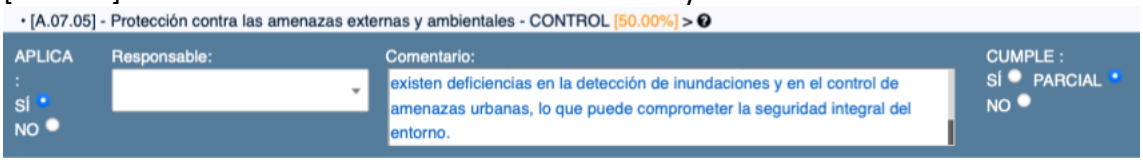
La seguridad de oficinas y espacios de trabajo es crucial para proteger la información confidencial y garantizar la integridad de las operaciones. Las directrices establecidas buscan limitar el acceso no autorizado y proteger la información sensible de miradas indiscretas, lo que puede prevenir potenciales violaciones de seguridad y filtraciones de datos.

- [A.07.04] - Control de la seguridad física



El control de la seguridad física en Mapfre se enfoca en establecer medidas robustas para proteger las instalaciones y los activos de información. Esto incluye el uso de sistemas de vigilancia, control de accesos y cumplimiento de normativas de protección de datos. Sin embargo, existen áreas donde el cumplimiento es parcial, lo que puede dejar brechas en la seguridad física.

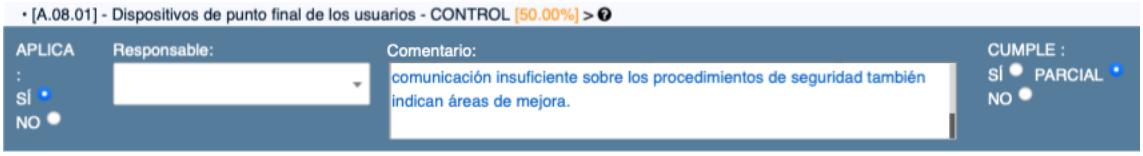
- [A.07.05] - Protección contra las amenazas externas y ambientales



El control de protección contra amenazas externas y ambientales se considera esencial para la continuidad y seguridad de las operaciones. Este control abarca desde la identificación de riesgos hasta la implementación de medidas de protección adecuadas, pero la ejecución puede ser inconsistente. Si bien se realizan algunas evaluaciones de riesgos y se toman medidas para amenazas como incendios y sobretensiones eléctricas, existen deficiencias en la detección de inundaciones y en el control de amenazas urbanas, lo que puede comprometer la seguridad integral del entorno.

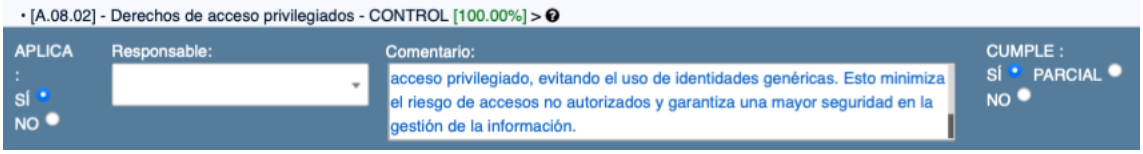
D) Tecnologia

- [A.08.01] - Dispositivos de punto final de los usuarios



Mapfre cumple parcialmente con el control A.08.01. Aunque ha establecido políticas sobre la configuración y manejo de dispositivos finales, algunos aspectos, como la separación entre el uso personal y profesional de dispositivos y la gestión efectiva de software, pueden no estar completamente implementados. La falta de seguimiento en la aplicación de salvaguardias técnicas adicionales para información sensible y una comunicación insuficiente sobre los procedimientos de seguridad también indican áreas de mejora.

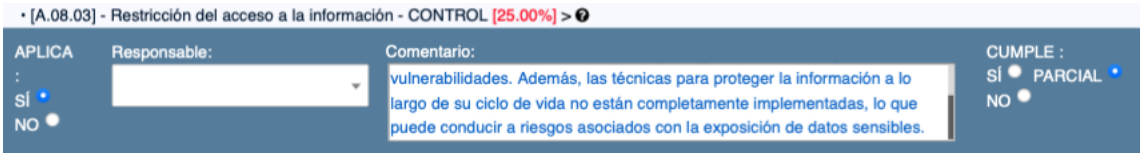
- [A.08.02] - Derechos de acceso privilegiados



Mapfre cumple con el control de derechos de acceso privilegiados. La organización ha establecido políticas claras para la asignación y gestión de accesos privilegiados, asegurando que estos sean otorgados únicamente a los usuarios que realmente los necesitan y que poseen las competencias adecuadas. Además, se realizan auditorías regulares para verificar la vigencia de estos derechos y se utilizan identidades

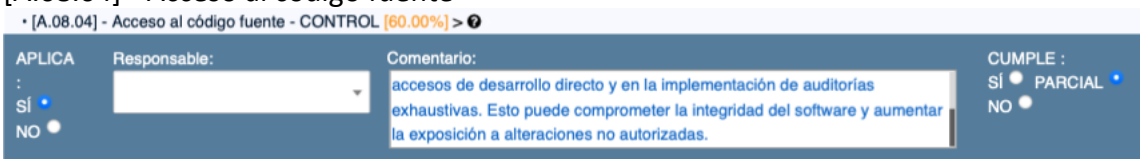
específicas para el acceso privilegiado, evitando el uso de identidades genéricas. Esto minimiza el riesgo de accesos no autorizados y garantiza una mayor seguridad en la gestión de la información.

- [A.08.03] - Restricción del acceso a la información



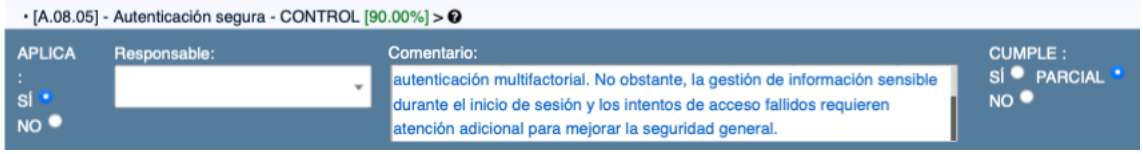
Mapfre cumple parcialmente con el control de restricción del acceso a la información. Si bien se han establecido políticas y mecanismos de control, la falta de implementaciones completas en gestión de acceso dinámico, así como en la protección de datos a lo largo de su ciclo de vida, limita la eficacia del control. Además, las restricciones de acceso en ciertos contextos y la falta de registros adecuados pueden incrementar el riesgo de exposición a datos sensibles.

- [A.08.04] - Acceso al código fuente



Mapfre presenta un cumplimiento parcial de este control. Aunque se han establecido políticas para controlar el acceso al código fuente y se utilizan sistemas de gestión de código, persisten deficiencias en el manejo de accesos de desarrollo directo y en la implementación de auditorías exhaustivas. Esto puede comprometer la integridad del software y aumentar la exposición a alteraciones no autorizadas.

- [A.08.05] - Autenticación segura



Mapfre cumple en gran medida con el control de autenticación segura, utilizando múltiples métodos de autenticación que incluyen biometría y autenticación multifactorial. No obstante, la gestión de información sensible durante el inicio de sesión y los intentos de acceso fallidos requieren atención adicional para mejorar la seguridad general.

7. Análisis de riesgos

Organizativos

- [A.05.01] - Políticas de seguridad de la información

  El riesgo asociado a la política de seguridad de la información se clasifica como medio debido a las áreas donde el cumplimiento es parcial, lo que podría resultar en vulnerabilidades. Se recomienda a Mapfre que implemente un plan de mejora continua y realice formaciones periódicas al personal para asegurar una comprensión y aplicación efectivas de la política.

- [A.05.02] - Roles y responsabilidades de seguridad de la información
  El riesgo asociado a la falta de claridad en roles y responsabilidades de seguridad es medio. Esto se debe a la posibilidad de errores en la gestión de la seguridad de la información, lo que podría conducir a incidentes de seguridad. Se recomienda a Mapfre implementar un programa de formación y documentación detallada para asegurar que todos los empleados comprendan y asuman sus responsabilidades, minimizando así este riesgo.

- [A.05.03] - Segregación de tareas
  El riesgo asociado a la falta de una adecuada segregación de tareas en Mapfre es medio, ya que la posibilidad de colusión y la asignación de roles conflictivos pueden llevar a incidentes de seguridad. Se recomienda implementar herramientas automatizadas para la gestión de roles y mejorar la supervisión de las actividades, asegurando así un control más efectivo sobre las funciones críticas.

- [A.05.04] - Responsabilidades de gestión
  El cumplimiento parcial del control [A.05.04] en Mapfre indica un riesgo medio alto. La falta de formación continua y de canales adecuados para la denuncia de violaciones puede resultar en una falta de concienciación entre los empleados, lo que aumenta la probabilidad de incidentes de seguridad. Para mitigar este riesgo, se recomienda implementar un programa robusto de formación y concienciación en seguridad, así como establecer mecanismos confidenciales de denuncia, asegurando que el personal se sienta apoyado y capacitado en su responsabilidad sobre la seguridad de la información.

- [A.05.05] - Contacto con las autoridades
  El riesgo asociado con el cumplimiento parcial de este control es medio, ya que la falta de claridad en los procedimientos de contacto con las autoridades puede resultar en respuestas inadecuadas ante incidentes de seguridad. Se recomienda que Mapfre desarrolle y documente un protocolo específico que detalle cuándo y cómo notificar a las autoridades, asegurando así una respuesta efectiva y en conformidad con las normativas aplicables.

Personas

- [A.06.01] - Investigación de antecedentes
  El riesgo asociado a la investigación de antecedentes en Mapfre es medio debido a las inconsistencias en la implementación de los controles, lo que puede dar lugar a la contratación de personal no completamente verificado, poniendo en riesgo la seguridad de la información. Recomendación: Mapfre debería establecer procesos más robustos y consistentes para garantizar que todas las investigaciones de antecedentes sean realizadas de manera efectiva y cumpliendo con las normativas vigentes, así como mejorar la capacitación del personal encargado de estas tareas.

- [A.06.02] - Términos y condiciones de empleo
  El riesgo asociado con este control se clasifica como medio, dado que la falta de claridad en las responsabilidades puede resultar en brechas de seguridad. Se

recomienda fortalecer la capacitación sobre las responsabilidades de seguridad y mejorar la comunicación en la fase de contratación para mitigar este riesgo.

- [A.06.03] - Conciencia, educación y capacitación en seguridad de la información
  Mapfre cumple parcialmente con este control, presentando un riesgo medio. Aunque existe un programa de capacitación en seguridad de la información, las áreas de evaluación continua de la comprensión del personal y la actualización de métodos de capacitación podrían ser mejoradas. Esto puede resultar en una preparación inadecuada ante amenazas emergentes. Se recomienda implementar un sistema más robusto para evaluar la efectividad del programa y diversificar los métodos de capacitación.

- [A.06.04] - Proceso Disciplinario
  Mapfre cumple parcialmente con el control, ya que hay áreas en las que la respuesta disciplinaria no es clara o efectiva, lo que puede generar un riesgo medio. Esta situación puede provocar que las infracciones a la política de seguridad no sean tomadas con la seriedad requerida, permitiendo que situaciones graves ocurran sin consecuencias adecuadas. Se recomienda implementar un sistema más robusto de seguimiento y evaluación de infracciones, así como la capacitación continua del personal para asegurar que las políticas sean respetadas.

- [A.06.05] - Responsabilidades ante la finalización o cambio
  El cumplimiento parcial de este control genera un riesgo medio, ya que la falta de un proceso claro para la transferencia de responsabilidades puede resultar en la pérdida de información crítica o en el acceso no autorizado a datos sensibles. Se recomienda establecer protocolos bien definidos para asegurar la correcta transferencia de roles y la comunicación efectiva de cambios operativos, minimizando así el riesgo asociado.

Infraestructuras

- [A.07.01] - Perímetro de seguridad física
  Mapfre cumple parcialmente con este control, ya que ha establecido algunas medidas de seguridad física, pero existen áreas donde la implementación es inconsistente o incompleta. Esto podría exponer a la organización a un riesgo medio, especialmente si las medidas de protección en puertas y ventanas no se aplican de manera uniforme. Se recomienda realizar auditorías periódicas para asegurar que todos los puntos vulnerables sean identificados y rectificados, fortaleciendo así la seguridad integral de las instalaciones.

- [A.07.02] - Entrada física
  Mapfre cumple de forma parcial con el control [A.07.02]. Aunque se implementan algunas medidas de control, hay áreas críticas como el acceso de visitantes y la gestión de entregas donde no se cumplen las directrices adecuadamente. Esto conlleva un riesgo medio-alto en términos de seguridad física, dada la posibilidad de accesos no autorizados o compromisos en la seguridad de la información. Se recomienda realizar una auditoría exhaustiva de los procesos de control de acceso y mejorar la formación del personal en procedimientos de seguridad.

- [A.07.03] - Seguridad de oficinas, despachos y recursos
  Mapfre cumple parcialmente con este control, ya que, aunque se han implementado medidas para proteger la información confidencial, es posible que algunas instalaciones no sean lo suficientemente discretas y que ciertos documentos internos puedan estar accesibles a personal no autorizado. Esto genera un riesgo medio alto en términos de seguridad física. Se recomienda llevar a cabo una revisión exhaustiva de las medidas de seguridad en todas las oficinas y asegurarse de que se minimicen las indicaciones sobre actividades de tratamiento de información sensibles.

- [A.07.04] - Control de la seguridad física
  El cumplimiento de Mapfre con el control de seguridad física es parcial, especialmente en la protección de los sistemas de vigilancia y la gestión de alarmas, lo que presenta un riesgo medio-alto. Este riesgo se origina por la posibilidad de accesos no autorizados a las grabaciones y la falta de cobertura completa de alarmas. Se recomienda realizar una auditoría exhaustiva y mejorar la capacitación del personal sobre la gestión y supervisión de estos sistemas para reducir la exposición a vulnerabilidades.

- [A.07.05] - Protección contra las amenazas externas y ambientales
  El cumplimiento parcial del control por parte de Mapfre se traduce en un riesgo medio-alto debido a las vulnerabilidades en la gestión de inundaciones y en la evaluación de amenazas urbanas. Esta situación podría resultar en interrupciones operativas y daños a la infraestructura. Se recomienda implementar un plan de gestión más riguroso que incluya medidas específicas para mitigar los riesgos de inundaciones y mejorar la seguridad ante amenazas urbanas, asegurando así una protección integral.

Tecnologia

- [A.08.01] - Dispositivos de punto final de los usuarios
  El riesgo asociado al cumplimiento parcial del control A.08.01 es medio-alto, dado que la falta de implementación completa de las directrices puede exponer a la organización a vulnerabilidades en la seguridad de la información. Se recomienda a Mapfre fortalecer su capacitación al personal en los requisitos de seguridad y realizar auditorías periódicas para asegurar el cumplimiento de las políticas establecidas.

- [A.08.02] - Derechos de acceso privilegiados
  El cumplimiento de este control por parte de Mapfre presenta un riesgo bajo. A pesar de que se implementan las políticas adecuadas para la gestión de derechos de acceso privilegiados, el riesgo se mantiene debido a posibles brechas en la revisión y actualización continua de privilegios. Se recomienda fortalecer la automatización de la gestión de accesos para garantizar que todos los cambios organizativos se reflejen de manera oportuna en los derechos de acceso, minimizando así las vulnerabilidades.

- [A.08.03] - Restricción del acceso a la información
  El riesgo asociado a la restricción de acceso a la información en Mapfre se clasifica como medio. Esto se debe a la implementación parcial de controles críticos y a la falta de un enfoque dinámico para la gestión de acceso. Se recomienda que Mapfre

refuerce sus políticas de acceso y los procesos de monitoreo para asegurar la protección adecuada de la información sensible y mitigar el riesgo de posibles brechas de seguridad.

- [A.08.04] - Acceso al código fuente
  El riesgo de acceso no controlado al código fuente en Mapfre se clasifica como medio. Esto se debe a que, aunque existen medidas de seguridad, la falta de controles adecuados para el acceso directo de los desarrolladores y la insuficiencia en la auditoría de accesos pueden permitir alteraciones no autorizadas. Recomendación: Implementar un sistema de gestión de acceso más estricto que limite el acceso directo y que integre auditorías regulares para asegurar la integridad del código.

- [A.08.05] - Autenticación segura
  El riesgo asociado al control de autenticación segura en Mapfre es bajo. A pesar de las implementaciones efectivas de autenticación, se recomienda fortalecer los procedimientos relacionados con intentos de acceso no autorizados y mejorar la capacitación en el manejo de credenciales.

8. Conclusiones

MAPFRE revela una serie de áreas críticas en la gestión de la seguridad de la información que presentan riesgos clasificados principalmente como medios y medios-altos. En el ámbito organizativo, se identifican deficiencias en la claridad de roles y responsabilidades, la segregación de tareas y la formación del personal, lo que sugiere la necesidad de un programa robusto de capacitación y documentación. La seguridad física también muestra vulnerabilidades, especialmente en los controles de acceso y la protección contra amenazas ambientales, lo que requiere auditorías y mejoras en la formación del personal. En términos tecnológicos, se destacan riesgos relacionados con la gestión de accesos, la restricción de información y la protección del código fuente, sugiriendo la implementación de controles más rigurosos y auditorías regulares. En general, se recomienda a MAPFRE adoptar un enfoque de mejora continua que incluya formación, documentación adecuada y protocolos claros para mitigar estos riesgos y fortalecer la seguridad de la información.

9. Bibliografía

- https://ar.emarisma.com/respuesta/index/15112?tab=2
- https://www.mapfre.es/particulares/
- https://www.iso.org/standard/27001
- https://www.normas-iso.com/iso-27001/
- https://areadeclientes.mapfre.es/login/particulares
- https://www.aenor.com/salainformaciondocumentos/NP-Mapfre%20ISO-IEC%2027001%20oct-19.pdf

- https://www.einforma.com/informacion-empresa/mapfre-familiar-compania-seguros-reaseguros
- https://ine.es