Política de seguridad[1]

MACCORP EXACT CHANGE, E.P., S.A.[2]

Versión	Elaboración	Aprobación	Entrada en vigor
1.1	Informática, Legal Operaciones y Cumplimiento	Dpto. Legal.	1.1.18
1.2	Ídem	Consejo de Administración	1.9.18

[1] En lo sucesivo, **PS**.
[2] En adelante, **Maccorp** o la **Entidad,** indistintamente.

SUMARIO

ACLARACIÓN PREVIA

A la fecha de la aprobación del presente documento, ***Maccorp todavía NI permite a sus clientes la realización de pagos electrónicos NI ha autorizado la emisión de tarjetas de ningún tipo que operen contra las cuentas de pago****. Esto significa que una parte muy importante de los preceptos de PSD 2 en la materia de seguridad electrónica -para pagos basados en tarjeta o de simple transferencia de crédito- no resultan aplicables, o al menos* ***no*** *lo resultan en los términos establecidos en dicho instrumento legal. Sin perjuicio de tal hecho, Maccorp ha establecido una muy estricta política de seguridad para la oferta actual de servicios de pago -como se podrá observar en el presente documento- de tal manera que cuando la evolución del negocio lo indique, se pueda realizar la transición de forma no traumática hacia la ejecución directa de pagos electrónicos. Descrita de manera simple, en la actualidad la ejecución de servicios de pago por Maccorp exige que el cliente o bien se persone en nuestras oficinas o bien nos comunique por procedimientos electrónicos, telefónicos u otros habilitados los datos del pago a ordenar, de tal forma que Maccorp los ejecuta per se -y* ***siempre después de haberlos confirmado telefónicamente por segunda vez****-.*

1. INTRODUCCIÓN

La Directiva UE 2015/2366[3], del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, de servicios de pago en el mercado interno[4], que reforma las Directivas 2002/65/EC, 2009/110/EC y 2013/36/EU y el Reglamento UE 1093/2010, y deroga la Directiva 2007/64/EC, ha establecido un nuevo conjunto de requisitos de autorización de Entidades de Pago[5].

En efecto, **el artículo 5 de la Directiva**[6] establece, entre otros: "*1. A los efectos de la obtención de autorización como EP, el solicitante remitirá oportuna solicitud a las Autoridades Competentes de su Estado Miembro, acompañada de los siguientes documentos: ….j) un documento que contenga la* ***política de seguridad****, incluyendo una detallada evaluación del riesgo en relación con los servicios de pago, así como una descripción de los controles de seguridad y de las medidas de mitigación implementadas para proteger adecuadamente a los usuarios de los servicios de pago contra los riesgos identificados, incluyendo el fraude y el uso ilegal de datos sensible y personales…".*

Dado que este novedoso requisito de autorización es también requisito de mantenimiento de la licencia, el presente procedimiento -de cumplimiento obligatorio y entrada en vigor inmediata- tiene el objetivo establecer la PS de Maccorp.

[3] En adelante, la Directiva o PSD2, indistintamente.
[4] Desarrollada, adicionalmente, a través del Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017, que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo, en relación con los estándares técnico-regulatorios para la autenticación de usuarios y para los estándares abiertos de comunicación comunes y de seguros.
[5] En adelante, EP o EPs -singular o plural-.
[6] Sobre solicitudes de autorización.

2. DEFINICIONES

Resultan de aplicación al presente procedimiento las siguientes definiciones:

a) **Incidente -operativo o de seguridad[7]-**: Un evento particular o una serie de eventos vinculados no planificados que tengan o puedan tener un impacto negativo en la *integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad* de los servicios relacionados con el pago[8].

b) **Incidente de seguridad[9]:** A los efectos de este documento, se considerará **incidente de seguridad** a toda potencial acción[10] que pretenda o intente, directa o indirectamente, la alteración de cualquiera de las características *cualitativas* de los servicios de pago, incluidas las asociadas a sus soportes técnicos, en la medida en que pudieran a las ya citadas características -es decir, a la **integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad**-. Los incidentes de seguridad se clasificarán causalmente en alguno de los siguientes tipos:

Concepto[11]	Características
Ataque externo	La causa desencadenante del IS está en el exterior, está dirigida deliberadamente contra la Entidad y es intencionalmente malicioso (por ejemplo, intento de penetración con troyanos, o con *software* que pueda robar datos o tomar el control de procesos, ciberataques de distintos tipos, etc.)
Ataque interno	La causa desencadenante del IS está en el interior, está dirigida deliberadamente contra la Entidad y es intencionalmente malicioso (por ejemplo, intento de penetración con troyanos por un empleado o colaborador, o con *software* que pueda robar datos o tomar el control de procesos aprovechando el conocimiento interno que el colaborador pudiera haber obtenido, etc.)
Evento externo	Por ejemplo, desastres naturales, asuntos legales, cuestiones comerciales y dependencias del servicio, etc.
Error humano	El incidente es causado por el error involuntario de una persona, ya sea como parte del procedimiento de pago (por ejemplo, cargar un lote de pagos erróneo en el sistema

[7] IOS.
[8] También identificables como las **características cualitativas** de la información asociada a la prestación de servicios de pagos.
[9] IS.
[10] En particular, **acceso, uso, revelación, interrupción, modificación o destrucción no autorizada de los activos, registros y órdenes.**
[11] Puede estar en investigación.

	de pagos) o porque esté relacionado con él de alguna manera (por ejemplo, la electricidad se corta accidentalmente y la actividad de pago queda retenida)
Fallo del proceso	La causa del incidente ha sido una deficiencia en el diseño o la ejecución del proceso de pago, los controles del proceso o los procesos de soporte (por ejemplo, proceso de cambio/migración, pruebas, configuración, capacidad, seguimiento)
Fallo del sistema	La causa del incidente está asociada con un diseño, una ejecución, unos componentes, unas especificaciones, una integración o una complejidad inadecuados de los sistemas que soportan la actividad de pago
Otros	La causa del incidente no es ninguna de las anteriores

En el caso de ataques, adicionalmente, deberán ser clasificados a su vez en alguno de los siguientes tipos:

Tipo de ataque[12]	Características
Denegación de servicio/distribuida (D/DoS)	Intento de impedir la disponibilidad de un servicio on line sobrecargándolo con tráfico procedente de múltiples fuentes
Infección de los sistemas internos	Actividad dañina que ataca los sistemas informáticos, tratando de robar espacio en el disco duro o tiempo de la CPU, acceder a información privada, corromper datos, robar contactos, etc.
Intrusión dirigida	Acto no autorizado de espionaje, intromisión (*snooping*) y robo de información a través del ciberespacio
Otros tipos de ataque	Cualquier otro tipo de ataque que se pueda haber sufrido, ya sea directamente o a través de otro proveedor de servicios, en particular, si se ha sufrido un ataque dirigido contra el proceso de autorización y autenticación

c) **Riesgo de seguridad:** Riesgo resultante de la inadecuación o fallo de procesos internos o de sucesos externos que tengan o pudieran tener un impacto negativo en la disponibilidad, integridad o confidencialidad de los sistemas de información y comunicación y/o de la información utilizada para la prestación de servicios de pago. Este riesgo **incluye** el riesgo de **ciberataques** o el riesgo derivado de una seguridad **física inadecuada**.

d) **Integridad**: Propiedad de salvaguardar la exactitud y la integridad de los activos (incluidos los datos).

[12] Puede estar en investigación, al igual que puede ser multi-causal.

e) **Disponibilidad**: Propiedad de garantizar la disponibilidad y la capacidad de utilizar los servicios relacionados con el pago por parte de los usuarios de servicios de pago.

f) **Confidencialidad**: Propiedad de que la información no se ponga a disposición de terceros, entidades o procesos no autorizados, ni se divulgue a dichas personas, entidades o procesos.

g) **Autenticidad**: Propiedad de que una fuente sea lo que afirma ser.

h) **Continuidad**: Propiedad de que los procesos, las tareas y los activos de una organización necesarios para la prestación de servicios relacionados con el pago sean plenamente accesibles y se ejecuten a niveles predefinidos aceptables.

i) **Servicios relacionados con el pago**: Toda actividad empresarial en virtud del artículo 4, apartado 3, de la PSD2 y todas las tareas técnicas de apoyo necesarias para la correcta prestación de servicios de pago.

j) **Identificación electrónica**: el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica

k) **Medios de identificación electrónica**: una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.

l) **Datos de identificación de la persona**: un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica.

m) **Sistema de identificación electrónica**: un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a

las personas físicas o jurídicas o a una persona física que representa a una persona jurídica.

n) **Autenticación**: un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.

3. FUENTES NORMATIVAS

Las fuentes legales del presente procedimiento son:

a) **La** -ya citada- **Directiva UE 2015/2366**[13]**, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, de servicios de pago en el mercado interno**[14], que reforma las Directivas 2002/65/EC, 2009/110/EC y 2013/36/EU y el Reglamento UE 1093/2010, y deroga la Directiva 2007/64/EC.

b) El ya citado **Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017,** que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo.

c) El **Reglamento UE 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014**, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

d) La **Guía EBA GL/2017/10**, sobre reporte de incidentes.

e) La **Guía EBA GL/2017/17**, sobre medidas de seguridad.

f) La **Guía EBA GL/2017/09**, sobre autorización de EPs.

g) La **Guía EBA GL/2014/12**, sobre seguridad de los pagos por Internet.

h) La **Guía EBA GL/2018/05**, sobre reportes de fraude.

i) **Cualesquiera otros instrumentos jurídicos** emitidos por las Autoridades Competentes, tanto del Reino de España como de la UE, con contenidos relevantes a los efectos de este procedimiento.

[13] En adelante, la Directiva o PSD2, indistintamente.
[14] Desarrollada, adicionalmente, a través del Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017, que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo, en relación con los estándares técnico-regulatorios para la autenticación de usuarios y para los estándares abiertos de comunicación comunes y de seguros.

Desde el punto de vista técnico, este procedimiento incluirá los **estándares técnicos** -en la medida en que no colisiones con ninguno de los preceptos jurídicos del párrafo anterior- que establecen los siguientes instrumentos: ISO 27000[15]; UNE-ISO/IEC 27001:2007 "*Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos*[16]"; ISO/IEC 27002[17]: (anteriormente denominada ISO 17799); ISO/IEC 27003[18]; ISO 27004, publicada en diciembre de 2009, que especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados; ISO 27005, publicada en junio de 2008 y que incluye una guía para la gestión del riesgo de la seguridad de la información[19]; e, ISO 27006, publicada en febrero de 2007, que especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

[15] Publicada en mayo de 2009. Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000.
[16] Fecha de la de la versión española: 29 noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. Contempla los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799).
[17] Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con **11 dominios, 39 objetivos de control y 133 controles**.
[18] Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
[19] Sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

4. OBJETIVO DE ESTE DOCUMENTO

El objetivo de este documento es establecer con **el máximo rigor** la **PS corporativa** de Maccorp. En consecuencia, sus reglas resultan de **aplicación obligatoria** por todos los empleados, directivos o colaboradores.

La ejecución efectiva de esta PS incluye **la coordinación ejecutiva** con otras reglas y procedimientos internos, y en particular con los siguientes:

a) **Procedimientos de detección, gestión y comunicación de incidentes operativos o de seguridad.**
b) **Procedimiento de supervisión, tramitación y seguimiento de incidentes de seguridad.**
c) **Procedimiento de recopilación de datos estadísticos de rendimiento, transacciones y fraude.**
d) **Reglas de continuidad de negocios.**

5. ALCANCE DEL DOCUMENTO

La PS de Maccorp se aplica a todos los medios, datos e información en poder de la compañía relacionada con la prestación de los servicios de pago[20], incluida la de mero soporte. También quedan incluidos todos los medios de ejecución de tales, incluidos los activos asociados. En consecuencia, quedan afectados a la presente PS y cada uno de los **activos informáticos** que desarrollan, o soportan, todos y cada uno de los servicios de pago de la Entidad, **incluyendo** datos, aplicaciones, sistemas operativos y otro *software* de base, *hardware*, telefonía y electrónica de red, así como los servicios informáticos y de telecomunicaciones prestados por terceros -o a terceros[21]- en la medida en que estén relacionados con cualquiera de los anteriores.

[20] Incluyendo la generada por Maccorp a los efectos de la identificación y autenticación de usuarios.
[21] Incluidos otros prestadores de servicios de pago.

6. MODELO ORGANIZATIVO

La distribución interna de competencias queda asignada de acuerdo con los principios de **jerarquía, responsabilidad, coordinación, prudencia, ejecutividad y eficiencia**.

6.a. Alta Administración

El Consejo de Administración es el órgano que lidera y establece **las políticas estratégicas en materia de seguridad informática** y conectadas. Asimismo, establece el nivel de riesgo tolerable[22], tanto en esta materia como en cualesquiera otras.

El **Director General** es responsable directo del seguimiento regular de la PS, así como de su mantenimiento actualizado y de la ejecución efectiva de las decisiones del Consejo de Administración en esta materia.

El Director General elevará al Consejo de Administración, tantas veces como sean necesarias, pero como mínimo una vez al año, informes sobre el estado de la PS, su calidad, su efectividad, así como los planes de mejora continuada. En dicho informe se evaluarán, necesariamente, los resultados obtenidos en los diferentes incidentes de seguridad y las *lecciones aprendidas*.

6.b. Comité de Tecnología, Seguridad y Continuidad de Negocio

El Comité de Tecnología, Seguridad y Continuidad de Negocio es el órgano de centralización del control de las tareas operativas y funcionales en esta materia. Estará constituido por el Director General -que será su presidente nato-, el Director de Informática y Sistemas -que será su secretario nato- el Jefe de Seguridad Informática, el Jefe del Departamento de Operaciones y la persona designada con funciones de jefatura de Riesgos o equivalente. Todos ellos podrán designar un sustituto para aquellas ocasiones en las que no puedan participar personalmente en las reuniones. Asimismo, podrán ser invitados a participar con voz y sin voto cuantos empleados o colaboradores se consideren oportunos, a los efectos de contribuir a mantener los más altos estándares de seguridad informática y antifraude.

[22] A pesar de ser equivalente, intentamos evitar el concepto "*apetito de riesgo*" pues podría resultar equívoco.

6.c. Departamento de Informática y Sistemas

A él corresponde la **responsabilidad operativa** respecto del riesgo informático. Desarrolla controles internos efectivos y ejecuta las políticas y procedimientos de manera continuada, incluyendo la supervisión de los riesgos correspondientes a las actividades de terceros[23]. Revisará, en particular, que todo contrato con terceros que incluya servicios informáticos incluya las medidas de seguridad apropiadas, como por ejemplo la firma de acuerdos de confidencialidad y el conocimiento por parte del personal externo afectado de las disposiciones de esta PS.

6.d. Jefe de Seguridad Informática

Estará encuadrado administrativamente dentro del Departamento de Informática y Sistemas y tendrá autoridad y control de los recursos necesarios para cumplir su función. Adicionalmente, actuará como delegado del Consejo de Administración a los efectos de la plena ejecutividad de las reglas de seguridad informática.

Sus funciones están descritas a lo largo del presente procedimiento e incluyen, en todo caso, las siguientes:

a) **Liderar las actuaciones diarias** que resulten necesarias para garantizar la efectiva implementación de esta PS.
b) **Proponer** las modificaciones que resulten necesarias, de acuerdo con los cambios normativos y las mejores prácticas de mercado, para mantener actualizada esta PS.,
c) **Realizar test periódicos internos** de control de la efectividad de la PS.
d) Coordinar la ejecución de **test de control externos**, incluyendo las auditorías en la materia.
e) **Organizar** los recursos asignados a la PS.
f) **Proponer** las reglas de gestión del riesgo de seguridad.
g) **Recibir** todas las comunicaciones relacionadas con esta política.
h) Instar la **revisión obligatoria** de la PS después de todo incidente de magnitud no trivial.

[23] Por tanto, quedan incluidos los empleados u otro personal al servicio de dichos terceros.

i) Actuar como **facilitador** de todas las comunicaciones corporativas en esta materia.
j) Actuar como **asesor** en esta materia del Director General y del Consejo de Administración.
k) Las restantes que son asignadas en este procedimiento.

7. SISTEMA DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO[24]

La entidad desarrolla un **Sistema de Gestión de la Continuidad de Negocio basado en la norma ISO 22301.** Este sistema incluye como estrategia de recuperación las siguientes consideraciones técnicas respecto de las prácticas actuales de copias de seguridad y recuperación ante desastre, e incluye características de alta disponibilidad de los servicios.

Almacenamiento

Los *backups* se almacenan en medios de almacenamiento en **Raid6** tanto para las copias *on site* como para las remotas. Estos medios de almacenamiento **no están conectados al dominio** y solo son accedidos por el *software* de copias de seguridad o con usuarios de administración locales. La copia local se encuentra en las oficinas de Maccorp y la copia remota se encuentra en la oficina de SOL.

Verificación y réplica

La réplica remota se envía *on line* a través de una **conexión cifrada** y tan pronto como se van generando las copias incrementales.

Los *backups* locales y remotos se verifican y re-verifican para la monitorización y el envío de alertas.

Recuperaciones

En caso de requerir la recuperación total o parcial de los datos, las copias de seguridad se pueden explotar y hacer operativas en cualquier punto de restauración en cuestión de segundos. Para realizar cualquier restauración es imprescindible disponer de la contraseña de cifrado.

Correo

Las cuentas de correo proveen una protección de 30 días de *backup* y **tres niveles de papeleras** donde se almacenan los elementos borrados. Dos de ellas accesibles para los usuarios y la tercera sólo por medio de asistencia técnica del fabricante.

[24] Véase documento especial de Política de Continuidad de Negocio a tal efecto.

8. RECUPERACIÓN ANTE DESASTRES

En caso de requerir la recuperación de un servidor completo se puede levantar cualquier punto de restauración con una **VM** con la tecnología *VirtualBoot* o en cualquier *Hypervisor* (HyperV, VmWare) en cuestión de minutos. Dependiendo de la gravedad del incidente y tras la valoración, se puede determinar la restauración de tres formas diferentes, a saber:

A. In situ, se realizaría sobre el equipo actual recuperándose todas las funcionalidades
B. Sobre un equipo de respaldo o nuevo, traspasando la copia existente y recuperando todas las funcionalidades
C. Nube, traslado del servicio necesario a la nube recuperando sus funciones

En caso de requerir una restauración *bare-metal*[25] se puede practicar casi sin *downtime* (tiempo de imposibilidad de uso) accediendo a la VM de restauración y con la tecnología HSR hasta replicar el servidor por completo antes de hacer el cambio.

En caso de desastre total se puede montar la copia remota en una VM en cuestión de minutos con la tecnología *VirtualBoot* o en un hipervisor. Mediante HSR se puede recuperar el servidor completo mientras se está trabajando sin *downtime*. Solo hay una interrupción cuando se decide pasar de "*modo desastre*" a "*modo normal*". Este *downtime* solo implica apagar el servidor virtual en "modo desastre" y el inicio del servidor recuperado.

[25] Sistema o red en la que una máquina virtual se instala directamente sobre el hardware en lugar de conectarlo con el Sistema Operativo.

9. COORDINACIÓN CON LAS POLÍTICAS Y PROCEDIMIENTOS DE NOTIFICACIÓN Y GESTIÓN DE INCIDENTES

Cuando sea detectado -o conocido- un incidente de seguridad, se alertará de **forma inmediata al Jefe de Seguridad Informática,** que será la autoridad interna responsable de la gestión y resolución, incluyendo la coordinación que resulte necesaria con otros Departamentos de la Entidad. En el desarrollo de tal función, el Jefe de Seguridad está autorizado a emitir instrucciones directas e inmediatamente ejecutivas a todos los empleados y colaboradores, sin perjuicio de su ulterior revisión y confirmación por parte del Comité de Tecnología, Seguridad y Continuidad del Negocio.

Una vez recibida la notificación del incidente de seguridad -bien automatizadamente, bien a través del personal o terceros- el Jefe de Seguridad iniciará las acciones de resolución que resulten necesarias. **En paralelo** se iniciarán las acciones establecidas en los siguientes procedimientos internos:

a) Los obrantes en el documento interno, en la medida que resulten aplicables, denominado, ***Procedimientos de administración integral de datos de pago calificados como sensibles y reglas anti-fraude, y***

b) Los obrantes en el documento interno, en la medida en que sean aplicables, denominado ***Procedimientos de detección, gestión y comunicación de incidentes operativos o de seguridad***.

10. POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE

Maccorp **prohíbe** la instalación y uso de *software* **no aprobado expresamente** por el Departamento de Informática y Sistemas. La descripción de los sistemas de IT autorizados y en uso se encuentra en el apartado séptimo de este documento**.** Para evitar esto, se ha establecido en el AD la política que lo impide y solo el personal de IT dispone de credenciales suficientes para poder llevar a cabo dicho cometido.

Los sistemas de Maccorp que son puestos a disposición de sus empleados, clientes y terceras partes se usarán **exclusivamente** para los propósitos de negocio de la Entidad y siguiendo todas las disposiciones de esta PS y sus actualizaciones. Su violación por parte de los empleados y colaboradores puede dar lugar a acciones disciplinarias y legales.

Todo el *software* instalado en los sistemas de Maccorp, incluidos los dispositivos de usuario final, servidores y ordenadores portátiles, deben disponer de la **licencia** correspondiente a nombre de Maccorp.

Las actualizaciones de los sistemas operativos se realizan **a diario y de forma automática**. En el caso de las estaciones de trabajo, son reiniciadas a diario por los usuarios en cada finalización de turno de trabajo. En el caso de los servidores, los reinicios son programados de forma manual en función de las ventanas de mantenimientos definida para cada uno de ellos.

Estas actualizaciones son monitorizadas, registradas y verificadas por **el programa de monitorización**, que es controlado por el Jefe de Seguridad Informática. En consecuencia, se mantiene un registro de las actualizaciones instaladas para su control inmediato, así como para su ulterior evaluación o informe.

11. POLÍTICA DE CONTROL DE CAMBIOS

Una parte fundamental de la **PS** de Maccorp, que merece especial atención, es el control de cambios. Así, se han establecido procedimientos que afectan tanto a los cambios en aplicaciones como en otros componentes o áreas de la organización, como bases de datos, *firewalls*, BCP (Plan de Continuidad del Negocio), etc.

Como principio esencial del control de cambios, su gestión se articula basándose en la diferenciación de roles y privilegios, estableciéndose así un flujo de aprobaciones necesarias para realizar dichos cambios, no siendo posible establecer caminos alternativos, excepto en los casos especificados en la gestión de crisis.

El proceso de cambios se analiza y se estudia caso a caso, y para implementarlo en los diferentes entornos se tienen en cuenta los diferentes tipos, ya sean de desarrollo o productivos. Es importante tener en cuenta que el *workflow* asociado a los entornos de desarrollo carece de algunas autorizaciones que son necesarias e imprescindibles para gestionar los cambios en los entornos productivos, dotando así de más agilidad en estos entornos.

Forma parte de la gestión de cambios la política de actualizaciones de aplicaciones y servidores, determinándose unos días concretos que se llevan a cabo mensualmente para su ejecución. La realización de cambios debe considerar la ejecución de las pruebas según lo dispuesto en la Sección 5.2.

Las áreas en las que se realizan más cambios y por lo tanto precisan de una herramienta de control son:

A. Herramientas de software para el desarrollo del negocio

Para todos los aplicativos que se desarrollan y utilizan para la realización de la actividad de negocio de MACCORP, establecen el registro de aquellos cambios que puedan afectar a datos importantes. Se ha de disponer de credencial suficiente para poder cambiar los datos. En la política de perfiles de usuario, se establece quien puede o no realizar cambios en según qué datos. Cuando un usuario autorizado procede a realizar una modificación de un dato, el sistema deja almacenada en la BBDD, toda la información correspondiente al cambio:

- Dato antiguo
- Dato nuevo
- Usuario que realizado el cambio
- Fecha / Hora cuando se produjo

B. Dpto. IT – Área de desarrollo de aplicaciones

Para gestionar los cambios sobre las aplicaciones desarrolladas, el Dpto. IT tiene un gestor GIT[26] donde se van almacenando todas las mejoras/modificaciones/nuevos procesos que se implantan sobre la o las herramientas para el desarrollo comercial de MACCORP.

11.a. Control de versiones y cambios

Cuando el Departamento de Informática y Sistemas realiza las modificaciones en los sistemas de Maccorp, procede a publicar la nueva versión para que las estaciones se actualicen automáticamente en el siguiente inicio. Los cambios son solicitados por los departamentos que se encargan, una vez realizados y actualizados, de verificar su correcto funcionamiento.

[26] Software de control de versiones, pensando en la eficiencia y la confiabilidad del mantenimiento de versiones de aplicaciones cuando éstas tienen un gran número de archivos de código fuente. Su propósito es llevar registro de los cambios y coordinar el trabajo que varias personas realizan sobre archivos compartidos.

12. POLÍTICA DE SEGURIDAD FÍSICA[27]

La seguridad de las instalaciones está diseñada **para impedir** el acceso físico no autorizado, así como daños físicos a los empleados, locales e información de Maccorp. Las medidas, políticas y procedimientos de seguridad se han diseñado teniendo en cuenta la proporción de riesgos y requisitos legales, normativos o contractuales asociados **a cada instalación**. El término "*instalación*", a los efectos del presente procedimiento, se refiere a cualquier local en el que se desarrollen actividades directas, indirectas, de soporte o conectadas con los servicios de pago prestados por Maccorp, y con completa independencia del estatus legal de dicha instalación -propiedad de Maccorp, en arrendamiento, etc.-.

A las instalaciones descritas en el párrafo anterior les resultan de aplicación los controles de seguridad física que mantienen la seguridad, tanto **perimetral** como **interna**, adecuada a las actividades comerciales realizadas en ellas. Los controles de seguridad que se aplican **prohíben el acceso no autorizado a las instalaciones**, además de proporcionar un mecanismo para notificar al personal cualquier intento de acceso no autorizado.

Los controles de seguridad **perimetral** disponibles en Maccorp **incluyen**:

1. Cerrado hermético de puertas y ventanas.
2. Alarmas de seguridad en puertas y ventanas.
3. Videovigilancia.
4. Sensores infrarrojos y/o de movimiento.
5. Alarmas contra incendios y sistemas de extinción de incendios.

En la sede central de Maccorp existe, asimismo, una sala refrigerada y con acceso restringido donde se colocan los *racks*[28] en los que se encuentran almacenados los dispositivos y equipos de la infraestructura tecnológica. La llave que da acceso a esta sala está custodiada por el departamento de IT y sólo tiene acceso a ella el personal expresamente autorizado.

[27] Dadas sus conexiones con la PS se incluyen las presentes normas de seguridad física.
[28] Armario metálico para agrupar las infraestructuras tecnológicas

Todo el equipamiento de IT distribuidos en oficinas externas y las distintas plantas de la casa central está protegido dentro de *racks* cerrados con llaves. Estas llaves están custodiadas por el departamento de IT (en la casa central) y por los responsables de cada oficina.

El servidor físico está protegido con un SAI[29] que le permite un apagado correcto en el caso de falla de suministro eléctrico, asegurando que no se pierda información. El servidor tiene configurado un RAID 6[30] tanto en los volúmenes de sistema como en el de datos que tolera la falla de hasta 2 de los discos que componen el RAID, esto quiere decir, que, si se diera un fallo físico en 1 o 2 discos del RAID, se podría o podrían sustituir por otro nuevo sin que esto supusiera la perdida de información, ni tendríamos que dejar de operar en ningún momento. Todos estos cambios de discos se pueden realizar con el servidor en funcionamiento de manera manual.

[29] Sistema de Alimentación Ininterrumpida
[30] Sistema de almacenamiento redundante de discos independientes

14. POLÍTICA DE SEGURIDAD DE CORREO ELECTRÓNICO

Maccorp utiliza los servidores de correo protegidos con una **conexión cifrada** y en la cual se gestiona la **primera capa** de seguridad **antes** de la entrada del correo en Maccorp.

El acceso a las cuentas se realiza mediante el cliente de correo, el cual se mantiene actualizado con la última versión disponible, con la finalidad de obtener la máxima protección posible en relación con vulnerabilidades que se vayan conociendo y resolviendo por parte de su desarrollador.

En Maccorp cada usuario cuenta con una **cuenta nominativa**, de tal forma que siempre está identificada la persona que envía, o recibe, correos electrónicos. Sobre tales usuarios se crean también otros, que son departamentales o asociados a servicios que pueden recibir y/o gestionar varias personas por medio de buzones compartidos y/o alias o listas de distribución.

Para todas las cuentas se han establecido las siguientes configuraciones de seguridad:

- Se ha aplicado una política de **expiración** en las contraseñas de los correos de 180 días.
- Cuenta con una fortaleza de, como mínimo, **8 dígitos** y recuerda las últimas tres claves utilizadas, de forma que no es posible repetirlas al momento de cambiarla.
- **No se permite** la utilización del nombre de la cuenta, apellidos o iniciales como parte de la contraseña.
- La contraseña debe tener **números, letras, mayúsculas, minúsculas y caracteres especiales**.
- Se encuentra permanentemente activada una funcionalidad de auditoría de accesos e intentos fallidos. La herramienta que proporciona de gestión el servidor de correo, permite extraer y monitorizar los intentos fallidos, así como los accesos llevados a cabo por cada cuenta.
- Bloqueo **automático** de cuentas ante múltiples intentos fallidos de inicio de sesión que se activa cuando se superan los 5 intentos.
- Se ha habilitado una política de detección de comportamientos sospechosos que incluye controles sobre las siguientes acciones:

- Múltiples intentos fallidos de inicio de sesión. Esta establecido por defecto, quedando en 3 intentos que una vez cumplidos deja inactivo el acceso por un tiempo de 5 minutos, volviendo a poder realizado pasado ese tiempo

- Política de anti-spam[31]. El servidor de Correo, facilita la comprobación previa contra listas de correo anti-spam para desestimar aquellos correos de procedencia dudosa.

Adicionalmente, resulta posible cifrar los correos y/o documentos adjuntos, según lo descripto en la **Política de Cifrado**[32].

[31] Método para prevenir el correo basura
[32] Ver **Capítulo 16** de este documento -Cifrado-.

15. POLÍTICA DE SEGURIDAD DE ACCESOS Y DE SEGURIDAD DE ÓRDENES DE PAGO[33]

En todos los casos los clientes -o candidatos a cliente- con cuenta de pago deberán aportar previamente al inicio de relaciones comerciales, **datos operacionales suficientes** para su **conocimiento** e **identificación indubitable**[34]. Dichos datos se podrán cumplimentar por métodos presenciales o remotos. A tal fin se utilizará el formulario obrante, se incluirán campos de datos independientes entre sí (**conocimiento, posesión e inherencia**[35]) que permitan, asimismo, la generación -de ser necesario- de claves adicionales de **autenticación** a ser utilizadas en los casos establecidos en este documento.

En ningún caso se podrán realizar operaciones, o acceso a datos, en modo remoto, sin acreditar fehacientemente la titularidad de la cuenta de pago, incluyendo en particular la acreditación del conocimiento sin error o duda de la **clave de acceso personal e intransferible** otorgada oportunamente[36].

Adicionalmente, en aquellos específicos casos que se establecen en este procedimiento para ciertas operaciones y servicios de pago iniciados por Maccorp se aplicarán **reglas reforzadas de autenticación** basadas en al menos dos elementos de los tres conceptos de seguridad suplementaria (**conocimiento, posesión e inherencia**) que resultan **exigibles** para la obtención de **claves operativas especiales**[37]. Sin aplicación de las reglas reforzadas de autenticación no se permitirá ni el acceso a las cuentas[38] ni la emisión de instrucciones de pago, en los casos así establecidos en este documento. En ningún caso podrán ser deducidas las informaciones asociadas a la aplicación de reglas reforzadas de autenticación a partir de la visualización o conocimiento de la clave de acceso ni se podrá generar una nueva clave de acceso a partir de una clave anterior.

---

[33] A estos efectos, distinguiremos entre los procedimientos establecidos con generalidad para los servicios de pago y los establecidos, específicamente, para los servicios de envío de dinero. Las reglas se aplican a ambos, salvo en los casos en los que específicamente se hace mención a los envíos de dinero y a reglas únicamente aplicables a éstos.

[34] Sin perjuicio de las reglas de PBCFT, protección de datos u otras aplicables.

[35] Este tercer concepto, por el momento, no resulta de aplicación.

[36] La negativa a cumplimentar el formulario implica la no aceptación de la relación comercial.

[37] **Adicionales a la clave general y específicas para cada transacción o acceso.**

[38] Con las excepciones establecidas en este procedimiento.

Se custodiarán con los máximos estándares de seguridad los datos asociados a los conceptos **conocimiento[39], posesión[40] e inherencia[41]**. En todo caso, antes de ser poder realizar una transacción para la que resulta exigible la obtención de una clave de asociados a los factores citados -al menos a dos de ellos-[42].

En los casos en que deban ser utilizadas **reglas reforzadas de autenticación adicional**, se cumplirán las siguientes reglas adicionales[43]:

a) Deberá insistirse al pagador, expresamente, respecto del importe del pago a realizar y de la identidad del receptor del pago.
b) El código de autenticación podrá ser utilizado, exclusivamente, para el importe originalmente comunicado y para la persona señalada con anterioridad como receptora del pago.
c) Cualquier modificación en el importe o el beneficiario implicará la no ejecución de la transacción y la necesidad de obtener un nuevo código de autenticación.

[39] Datos que **solamente el cliente conoce** -desde el nombre de su perro, a su lugar favorito de vacaciones, pasando por -por ejemplo- el nombre de su primer empleador u otros.
[40] Datos que **solamente el cliente posee**, como por ejemplo el resultado de la aplicación de una regla alfanumérica con una tabla en su poder.
[41] Datos **asociados al ser del cliente**, como por ejemplo resultados de lectores biométricos. En el caso de Maccorp **estos datos no serán por el momento objeto de explotación** ya que no se proveerá a los usuarios de aparatos o elementos de lectura o de interconexión para la ejecución de operaciones.
[42] Por defecto, se solicitarán los datos en un proceso único vía un formulario único, junto a la obtención de la clave general personal e intransferible del cliente, salvo decisión en contrario del Jefe de Seguridad.
[43] Además de reglas de seguridad que garanticen la confidencialidad, autenticidad e integridad de los datos de importe, beneficiario, así como cualquier otra información que sea desplegada en la pantalla transaccional, incluyendo los propios códigos de autenticación.

15.a. Ingreso al sistema[44]

Los servicios de pago se llevan a cabo a través de una plataforma **propiedad** de Maccorp. El *iter* operacional, desde el punto de vista del cliente, para el acceso al sistema operativo de Maccorp, es el siguiente:

a) El cliente cumplimenta los datos del formulario de alta y recibe, una vez hechas las comprobaciones y verificaciones necesarias, recibe por **medios seguros** un usuario y una contraseña[45]. Esta contraseña será válida por una sola vez y deberá ser modificada necesariamente por el cliente en su primer acceso remoto a la cuenta.
b) Para la activación de la cuenta, el usuario ingresa en nuestra plataforma, donde se le solicitará usuario y la contraseña genérica citadas en el punto anterior. Una vez aceptado, el cliente deberá proceder a modificar su contraseña.
c) Los accesos ulteriores se realizarán con el usuario entregado y la contraseña establecida por el propio cliente.
d) Si el cliente comete un error en los datos facilitados en el primer intento de acceso, el sistema indica el error, pero no ejecuta todavía acciones adicionales.
e) Si el cliente comete un segundo error al introducir los datos de usuario y contraseña, el sistema indica el **error** y procede a **bloquear** durante 5 minutos el acceso.
f) Si por tercera vez se vuelve a cometer un error en la introducción de datos, el sistema **bloquea indefinidamente** dicho usuario y lo pone en conocimiento de la División de Cuentas de Pago para que contacte con el cliente a fin de establecer la causa de los intentos fallidos. Si se confirma por el cliente que se ha tratado de su error, y a su solicitud, se reactiva el usuario teniendo que realizar los pasos descritos en los puntos anteriores.
g) En ningún caso se permitirán más de **tres intentos** de acceso.
h) En ningún caso se permitirán más de **cinco minutos** de inactividad.

[44] Posteriores a la comunicación de aceptación del cliente -en su caso- y con sujeción a la condición de cumplimentación íntegra del formulario para la obtención de clave personal e intransferible y de entrega de datos de conocimiento, posesión e inherencia, que podrán ser utilizados cuando corresponda, de acuerdo con la solicitud del cliente y las reglas operacionales de este documento.
[45] A solicitud del cliente podrá hacerse llegar el usuario y contraseña en soporte duradero seguro -por ejemplo, correo certificado- pero en ningún caso vía correo electrónico simple.

i) El cliente, titular de la cuenta, como usuario de la plataforma de Maccorp puede también administrar, crear o modificar todos los usuarios que precise[46], definiendo el nivel de acceso que tendrá cada uno. Asimismo, puede revocar los privilegios otorgados a los usuarios creados, anulando el perfil establecido.

15.b. Servicios de envío de dinero

El servicio de envío de dinero se realiza mediante la utilización de una **web propiedad de Maccorp**, que solicita usuario y contraseña **al propio empleado de Maccorp**, **confirmando** que el acceso se realiza a través de **un terminal ubicado físicamente** en las oficinas de Maccorp. En los casos excepcionales en los que se permita el **acceso remoto** a la instrucción de pagos en concepto de envío de dinero, se aplicarán las mismas reglas que en el caso de los servicios de pago generales con cuenta de pago.

15.c. Casos en los que no se requieren procedimientos reforzados de autenticación

Se requerirá la obtención de clave de autenticación p**ara todos los servicios electrónicos de pago iniciados[47] a través de la plataforma de Maccorp**, salvo en los casos siguientes[48]:

a) El acceso al saldo de la cuenta de pago, o de las cuentas de pago, en su caso.
b) El acceso al inventario de las transacciones de la cuenta durante los últimos 90 días.
c) El pagador inicia un pago electrónico de importe no superior a 50 euros, no existieran pagos por el mismo mecanismo superiores a 150 euros durante el período transcurrido desde la última fecha de acceso con uso de medios adicionales de autenticación y no se supere el número de 5 pagos[49].
d) El cliente haya comunicado una lista de beneficiarios de confianza y el pago sea destinado a una persona incluida en dicha lista, salvo en el caso de la creación o modificación de la citada lista[50].

[46] Especialmente, pero no solamente, en el caso de clientes personas jurídicas.
[47] Incluyendo el acceso a información.
[48] Con sujeción a la condición de restricción de acceso a datos sensibles -receptores, etc.-.
[49] Contados desde la última fecha de acceso con uso de medios de autenticación adicionales.
[50] Pues en estos casos, no obra la excepción.

e) El cliente haya comunicado y Maccorp haya constatado fehacientemente la existencia de una lista de beneficiarios recurrentes, salvo en el caso de la creación o modificación de la citada lista[51].
f) En los casos de movimientos entre cuentas del mismo cliente.
g) En los casos que califiquen como transacciones de bajo valor, en los términos establecidos en el artículo 16 del Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017, que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo[52].
h) En los casos de uso de protocolos a usuarios que carezcan de la calificación de **consumidores**, en la medida en que el nivel de protección sea al menos igual al establecido en el Ordenamiento Comunitario.
i) En el caso de terminales de aparcamiento sin empleados.
j) En el caso de terminales de autopista sin empleados.
k) En los casos en que así sea autorizado por la Autoridad Competente.
l) En los casos en los que la transacción que se pretende realizar sea **calificada en el nivel de riesgo -de seguridad- bajo.**

No obstante, las excepciones a) y b) no resultarán de aplicación ni en el primer acceso en línea a la cuenta ni en los casos en los que hubieran transcurrido más de 90 días desde el último acceso en línea a la cuenta -que hubiera requerido aplicación de las técnicas especiales de autenticación-.

15.d. Riesgo de seguridad bajo

Se clasificarán entre tales, aquellas transacciones en las que concurran todas las características siguientes:

a) La tasa de fraude para el tipo de transacción no supera los umbrales de la siguiente tabla[53]:

[51] No obra la excepción más que a partir del segundo, o ulteriores, pagos.
[52] El pagador inicia un pago electrónico de importe no superior a 30 euros, no existieran pagos por el mismo mecanismo superiores a 100 euros durante el período transcurrido desde la última fecha de acceso con uso de medios reforzados de autenticación y no se supere el número de 5 pagos durante idéntico plazo.
[53] Maccorp calculará sus propias tasas de fraude, en los términos establecidos en el artículo 19 del Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017, que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo. Este cómputo será auditado y

	Tasa de fraude en %	
Valor en euros	**E-pagos con tarjeta**	**E-transferencias de crédito**
500	0.01	0.005
200	0.06	0.01
100	0.13	0.015

b) Se cumplen los importes cuantitativos de la tabla anterior.

c) El programa de control **en tiempo real** de transacciones no detecta ninguna de las siguientes condiciones: gastos anormalmente altos, comportamiento inusual, infección durante la sesión por *malware*, esquema conocido de fraude, ubicación inusual del pagador o ubicación del pagador en territorio de alto riesgo.

d) En todo caso, se deberá haber valorado las siguientes características del pagador: patrón de conducta recurrente conocida, historial de pagos con diferentes proveedores de servicios, ubicación del pagador, ubicación del beneficiario si se le ha provisto de un instrumento de recepción de pagos por Maccorp e identificación de patrones de conducta anormal de pagos.

e) Todos los anteriores factores estarán incluidos en una tabla de puntaje que será revisada periódicamente.

15.e. Condición de utilización de excepciones[54]

El uso de las anteriores excepciones está condicionado, adicionalmente, a la monitorización y registro, por cada tipo de transacción, por períodos trimestrales, con separación de las transacciones presenciales y las no presenciales, de los siguientes datos:

a) Número de pagos en los que se aplica una excepción en relación al número total de pagos.

b) Valor medio de la transacción con excepción en relación con el valor medio de la transacción sin excepción.

c) Valor de las transacciones fraudulentas o no autorizadas en las que concurre excepción en relación con análogo valor de aquellas en las que no concurre excepción.

estará a disposición de las Autoridades Competentes. En caso de obtención de tasas superiores a los umbrales establecidos Maccorp cesará inmediatamente en la aplicación de esta excepción.

[54] Estarán a disposición de las Autoridades Competentes.

15.f. Confidencialidad e integridad de las claves de los clientes[55]

En todo caso, se deberán cumplir las siguientes condiciones respecto de tales claves:

a) Serán desplegadas con máscara, de tal forma que no puedan ser leídas en su totalidad en el proceso de autenticación del cliente.
b) En ningún caso se custodiarán como texto plano[56].
c) Todo material de uso criptográfico estará especialmente protegido contra su revelación o uso no autorizado.

El Jefe de Seguridad Informática establecerá las reglas y metodología criptográfica a establecer para garantizar el cumplimiento de los apartados anteriores. Adicionalmente, el Jefe de Seguridad Informática garantizará que:

a) Su generación[57] se realiza en un entorno seguro que cumpla las normas ISO, y
b) su procesamiento y envío[58] se realice a través de entornos seguros que cumplan las normas ISO.

En todo caso, Maccorp ha establecido mecanismos[59] que garantizan que solamente el usuario apropiado está asociado de manera segura[60] con sus claves personales y el *software* y el *hardware* de autenticación -en su caso, y de ser necesarios y entregados por Maccorp-. En todo caso, es relevante señalar que, por el momento, Maccorp no está entregando[61] -como consecuencia del modelo de negocio por el que ha optado el Consejo de Administración- ni *software* ni *hardware* de autenticación. En consecuencia, todas las referencias deben ser entendidas en relación con las claves personales y las de autenticación.

15.g. Medios seguros para la entrega, renovación, u otras acciones con claves personales

Se entenderá por medios seguros aquellos que cumplen las siguientes condiciones:

[55] Incluyendo los códigos de autenticación obtenidos por aplicación de técnicas reforzadas de autenticación.
[56] Ni las claves ni los datos que permiten obtenerlas.
[57] Tanto de las claves personales como de los códigos de autenticación.
[58] Tanto de las claves personales como de los códigos de autenticación.
[59] De acuerdo con las técnicas matemáticas de **correspondencia biunívoca.**
[60] Incluyendo la red de conexión.
[61] No es necesario pues el cliente ingresa en la plataforma de Maccorp, necesariamente.

a) mecanismos de entrega que garanticen que las claves se entregan al legítimo usuario, como por ejemplo correo certificado, entrega en mano a domicilio, exigencia de presencia en la sede de Maccorp, entrega notarial o equivalente, uso de firma electrónica, uso de sistemas gestionados por proveedores de seguridad certificados, etc.
b) En el caso de entrega **fuera de las oficinas** de Maccorp, no se entregará en ningún caso más de una copia y, adicionalmente, se exigirá la activación previa por medios remotos antes del inicio del uso.

En el caso de que cambie la política de Maccorp respecto de la entrega de *software* o *hardware*, adicionalmente, se establecerán mecanismos especiales de autenticación de dichos elementos antes de su uso.

A las **renovaciones** les resultarán de aplicación las mismas reglas que a las primeras obtenciones de claves. Asimismo, la destrucción, desactivación o revocación de las claves personales se realizará por **medios seguros**, de acuerdo con la definición anterior.

16. POLÍTICA DE CIFRADO

Maccorp establece en cada caso concreto, el cifrado para la comunicación de datos, atendiendo prioritariamente a la confidencialidad de la información a transmitir. En aplicación de este criterio, se establecen diferenciaciones que permite dirigir el tráfico de la información a través del conducto más apropiado para cada uso, la clasificación es:

Comunicación	Destino
VPN[62]	Oficinas propias remotas Entidades Financieras Corresponsales Pagadores
SFTP[63] / SSL	Entidades Financieras Corresponsales Pagadores
SSL[64]	Servidor WWW Cliente externo
TLS[65]	Email

[62] Virtual Private Network es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas y cifrado.

[63] Protocolo de transferencia de archivos que utiliza SSH (Secure Shell) para asegurar los comandos y los datos que se transfieren entre el cliente y el servidor, por lo que dejan de ser vulnerables a escuchas furtivas, interferencias o falsificaciones.

[64] "Secure Sockets Layer" protocolo que permitir que las aplicaciones transmitan la información de ida y vuelta de manera segura protegiendo su privacidad.

[65] Seguridad en la capa de transporte (TLS) es un protocolo de seguridad que cifra los correos para proteger la privacidad.

17. PROTECCIONES

17.a. Directorio activo

El acceso a todas las redes, sistemas, aplicaciones y bases de datos de Maccorp requiere una cuenta autorizada en **un dominio** ***Active Directory***[66]. Solo se proporciona el acceso mínimo necesario para que los usuarios puedan desempeñar las funciones que les correspondan.

Todas las cuentas de las redes, sistemas, aplicaciones y bases de datos de Maccorp garantizan cuentas asociadas a usuarios específicos y **no revelan** el nivel de acceso o el propósito de la cuenta.

17.b. Configuraciones de seguridad

Las cuentas de empleados tienen acceso a las redes, sistemas y aplicaciones de Maccorp según sea necesario. El acceso se proporciona mediante credenciales (ID de usuario y contraseña) que solo son conocidas por el **individuo asociado al ID de usuario.**

Para todas las cuentas se han establecidos las siguientes configuraciones de seguridad:

- Se ha aplicado una política de expiración en las contraseñas de 180 días.
- Cuenta con una fortaleza de mínimo 8 dígitos y recuerda las últimas tres claves utilizadas, de forma de no poder repetirlas al momento de cambiarla.
- No se permite la utilización del nombre de la cuenta, apellidos o iniciales como parte de la contraseña.
- La contraseña debe tener números, letras y, al menos, un símbolo.
- Auditoría activada de accesos e intentos fallidos
- Bloqueo automático de cuentas ante tres intentos fallidos de inicio de sesión por un tiempo determinado (15 minutos).
- Activadas los registros de auditoría de inicios y cierres de sesión.
- Se ha configurado la introducción de contraseña mediante un sistema de ofuscación, para que no sea posible visualizar los caracteres que se han introducido en la pantalla o formulario de acceso.

[66] Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

- Las contraseñas de inicio, emitidas para las cuentas de nuevos usuarios, vencen tras el primer uso, lo que obliga al usuario a establecer una nueva contraseña antes de completar el proceso de inicio de sesión.

17.c. Gestión de cuentas, claves y permisos

Las contraseñas emitidas por el personal autorizado de IT dedicado a la gestión del ***Directorio activo***, en respuesta a contraseñas olvidadas o cuentas de usuario bloqueadas, son proporcionadas al usuario d**e forma segura y solo después de que este haya proporcionado pruebas suficientes de su identidad** para poder emitir las nuevas contraseñas (DNI, número de teléfono de la empresa, verificación visual remota o presencial y de nombres y apellidos, etc.). Adicionalmente deberán ser autorizadas por el supervisor correspondiente. Deberán, asimismo, ser modificadas tras el primer acceso. Estas contraseñas una vez cambiadas o desbloqueadas son registradas en una **base de datos de incidencias**, junto al resto que se puedan producir**,** y notificadas a los responsables por correo electrónico.

Las solicitudes de acceso a las redes, sistemas, aplicaciones y bases de datos de Maccorp siguen un proceso **de escalado y aprobación** por los supervisores correspondientes. Así, el responsable del personal que solicita el acceso tiene que cursar una autorización.

Maccorp cuenta con un sistema para **modificar o retirar accesos** según sea necesario. Así, se está en proceso de automatización de los mecanismos para la eliminación de accesos, cuando surgen las siguientes circunstancias:

- Despido de empleados.
- Cambios en la función de trabajo de empleados.
- Interrupción de servicios de empleados.
- Finalización de servicios o salida de un usuario de un proyecto concreto.

Este sistema se basa en la agregación de grupos con permisos para acceder a la información o recursos necesarios, tras la creación de un nuevo usuario se agrega al correspondiente grupo o grupos para automatizar el proceso. En el caso de circunstancias anteriores será eliminado del grupo y deshabilitada la cuenta.

17.d. Administración de ordenadores

Las credenciales de acceso de administración de los ordenadores están **reservadas** al personal autorizado del departamento de IT. De esta forma se limita la posibilidad de los usuarios para instalar aplicaciones no autorizadas o realizar cualquier cambio en los equipos. La gestión de estos equipos se realiza de forma centralizada estando todos ellos unidos al ***dominio central***.

17.e. Entrega de claves a clientes

Véase capítulo 15 de este documento.

18. ESTÁNDARES DE COMUNICACIÓN SEGUROS

A continuación, se revisa, en el primer apartado, los mecanismos vigentes de comunicación con entidades financieras. Y en el segundo apartado se revisan los mecanismos diseñados -y en su caso, ya ejecutables- para los casos establecidos en el artículo 30 y siguientes del Reglamento Delegado de la Comisión 2018/389, de 27 de noviembre de 2017, que complementa la Directiva UE 2015/2366, del Parlamento Europeo y del Consejo.

18.a. Mecanismos ordinarios actuales de comunicación

MACCORP solamente interactúa con las entidades financieras[67]. para cada una de ellas se sigue un procedimiento diferente en la comunicación de las ordenes, detallamos las utilizadas:

TIPO DE COMUNICACIÓN	DESCRIPCIÓN
SFTP	**Comunicación de Operaciones**
	Cuando interviene para el intercambio de información con una entidad financiera, la utilización de ficheros, estos son depósitos en la dicha entidad. Para este funcionamiento, la entidad financiera facilita la siguiente información: 1. Dirección pública donde se encuentra el servicio 2. Usuario 3. Contraseña 4. Certificado que se descarga en la primera conexión para el cifrado de las comunicaciones. Los ficheros son confeccionados en la central e importados al SFTP a través de un aplicativo que valida con usuario y contraseña al encargado de enviar los ficheros siempre que tenga el privilegio establecido.
	Recepción de Errores
	A través de un aplicativo en central, se conecta con el SFTP utilizando las credenciales facilitadas por la entidad financiera, descargando los ficheros de respuesta depositados. Son procesados y enviado mail al responsable de los ficheros para que atienda los errores comunicados.

[67] Recuérdese que **no se ofertan, por el momento, operaciones automatizadas de pago ejecutadas directamente por los clientes.**

	Una vez subsanado el error, se procede a volver a comunicar la operación.
SSL	Se utilizan las plataformas Web de las entidades financieras para realizar las operaciones. Pueden realizarse de dos maneras: 1. Introduciendo en la banca electrónica los datos de la transacción a procesar utilizando los medios de validación propios de la entidad financiera 2. Subiendo un fichero que contenga las operaciones que se desean procesar En la misma plataforma se puede comprobar si se ha procesado el fichero, si ha contenido errores para subsanarlos y los comprobantes de cada una de las operaciones

18.b. Mecanismos especiales

Con la finalidad de permitir a los ASPSP[68], PISP[69] y PSPICPI[70] comunitarios prestar sus servicios respecto de la clientela con cuenta de pago abierta en MACCORP, en su caso y de acuerdo con la voluntad manifestada por el cliente, se oferta una *interface* que cumple las siguientes características[71]:

a) Los diferentes tipos de EPs citados en el párrafo anterior se podrán **identificar** a través de ella.
b) Se podrán realizar **comunicaciones** a través de ella.
c) Se podrán, en los casos autorizados, realizar **transacciones** a través de ella.
d) Los diferentes tipos de EPs citados podrán **descansar** en los procedimientos de autenticación accesibles vía la citada *interface*.
e) En particular, los diferentes tipos de EPs citados podrán a través de ella **instruir a MACCORP para que se inicie el procedimiento de autenticación**, de acuerdo con el consentimiento manifestado por el cliente; se mantendrán las sesiones de comunicación que resulten necesarias para el buen fin del servicio; y, la

[68] Entidades de pago con licencia para prestar servicios sobre dichas cuentas.
[69] Entidades de pago con licencia para iniciar servicios sobre dichas cuentas.
[70] Entidades de pago con licencia para emitir instrumentos de pago basados en tarjeta.
[71] Que en todo caso se ajustarán a los requerimientos emitidos por las organizaciones bien europeas bien internacionales de emisión de estándares.

confidencialidad e integridad están **estrictamente garantizadas** por MACCORP y la *interface* ofertada.

f) Se permitirá el acceso sin cargo de los citados prestadores de servicios de pago a los protocolos, rutinas y herramientas necesarias para garantizar la **interoperabilidad**[72].

g) En ningún caso se realizarán modificaciones de dicha interface sin que se ponga en conocimiento de los citados prestadores de servicios con **3 meses** de antelación, al menos[73].

h) Se facilitará el uso de un entorno de pruebas (*testing facility*) a los citados proveedores de servicios de pago con la finalidad de que puedan probar su *software* y aplicaciones de uso por sus clientes.

i) MACCORP proveerá de una **interface específica** -opción 1 del artículo 31 del Reglamento Delegado- a los citados proveedores de servicios de pago en condiciones de **disponibilidad, rendimiento y soporte idénticas** a las ofertadas a los clientes de pago[74]. En ningún caso se establecerán **obstáculos** de ningún tipo para el acceso y uso de dicha *interface* por parte de otras EPs[75].

j) Existirán **planes de contingencia** para los casos de imposibilidad de conexión por parte de otras EPs a dicha *interface*. A estos efectos, se entiende que demoras en la respuesta superiores a 30 segundos, o la ausencia de conexión real después de 3 intentos, son casos que implican necesariamente la activación de los citados planes de contingencia[76]. MACCORP permitirá, de acuerdo con dichos planes, que las **EPs se conecten a las mismas *interfaces*** que se utilizan para las relaciones con los clientes, mientras dura la imposibilidad de conexión a la *interface* habilitada especialmente para dichas EPs.

k) En los casos en los que resulten de aplicación los mecanismos excepciones establecidos en el punto anterior, MACCORP establecerá mecanismos y

[72] Además, se incluirá un resumen en el sitio web de MACCORP.
[73] Con la única excepción de situaciones de emergencia.
[74] En las condiciones establecidas en el artículo 36 de dicho Reglamento Delegado.
[75] Se monitorizará especialmente este hecho por parte del Departamento de Informáticas y Sistemas y se publicarán en el sitio web de MACCORP datos, estadísticas e indicadores de tales trabajos.
[76] Se harán públicos los mecanismos operativos asociados a dichos planes y se comunicará su inicio a las Autoridades Competentes.

controles que permitan asegurar que: (i) el acceso de las citadas EPs se limitará a aquellos datos estrictamente necesarios para la prestación de los servicios de pago autorizados y consentidos por el cliente, (ii) se cumple estrictamente con las obligaciones establecidas en los artículos 66 y 67 de PSD2, (iii) podrá poner el registro de accesos a disposición inmediata de las Autoridades Competentes, (iv) podrá justificar los accesos que hubieren existido a dichas Autoridades de manera inmediata y sin demora, y (v) podrá comunicarlos, en su caso, al resto de EPs.

l) Se utilizarán los **servicios de certificación** -a los propósitos de la identificación de EPs- establecidos en el **artículo 30, apartado 3 del Reglamente UE 910/2014.**

m) En todo caso, las sesiones se desarrollarán vía el uso extensivo de **técnicas criptográficas** robustas y aceptadas por la comunidad científica.

n) Resultarán de aplicaciones cualesquiera otras reglas técnicas dictadas por las Autoridades Competentes, autorizándose al Jefe de Seguridad a emitir *Circulares Internas de Seguridad* en las que puede establecer las normas que resulten apropiadas para la satisfacción de tales.

19. MONITORIZACIÓN DE LA SEGURIDAD

Es regla de obligado cumplimiento de Maccorp **la monitorización continuada** de **amenazas**, así como la evaluación periódica de **vulnerabilidades**, que puedan poner en peligro -siquiera contingentemente- la seguridad de los datos[77], activos, operaciones, u otros elementos necesarios para la correcta ejecución de los servicios de pago.

Regularmente se realizan controles de funcionamiento de los diversos sistemas que soportan la operativa y servicios prestados por Maccorp, entre las cuales figuran los análisis de vulnerabilidades generados **mensualmente**, y que derivan en acciones de cumplimiento para los diversos departamentos implicados. Sin perjuicio de tales existe un **control en línea de operaciones**, con utilización de un **algoritmo de riesgo**, que se describe a continuación.

Todas **las alertas de seguridad** a las que se hace referencia en este apartado son **recibidas por el Jefe de Seguridad Informática**, que las gestiona de manera inmediata; en caso de concurrencia de varios, las gestiona de acuerdo con el nivel asignado de prioridad. Asimismo, las registra en una **bitácora de control de seguridad**, de acuerdo con el formato establecido.

[77] Tanto estáticos como dinámicos.

20. APROBACIÓN, DIFUSIÓN Y ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD

La presente PS, y sus modificaciones posteriores, será aprobada por la Dirección General de la Entidad, que dará cuenta al Consejo de Administración a efectos de su ratificación, previa aprobación por el Comité de Tecnología, Seguridad y Continuidad del Negocio. A dicho Comité será presentado un borrador elaborado por el Jefe de Seguridad Informática.

Se distribuirá esta PS entre los empleados, clientes y proveedores de la Entidad que utilicen sistemas informáticos que estén dentro del alcance de la citada PS, de acuerdo con reglas prudenciales y de confidencialidad.

Esta PS permanecerá disponible y accesible en todo momento a través de la **Intranet** de la empresa y se reforzará su difusión y conocimiento **mediante cursos de formación internos.** Se realizarán controles periódicos para comprobar el nivel de conocimiento y sensibilización de la PS por el equipo de dirección de Maccorp y del resto de trabajadores de la compañía.

Adicionalmente, la Entidad buscará de manera activa la **concienciación de los clientes** respecto de los riesgos de seguridad y las acciones de reducción del riesgo.

Este documento deberá mantenerse **permanentemente actualizado**, reflejando la evolución del negocio, la innovación tecnológica y la identificación de nuevas vulnerabilidades y amenazas. El Jefe de Seguridad del Departamento de Informática y Sistemas revisará anualmente la PS y los documentos relacionados y propondrá, de ser necesario, modificaciones de la PS para su ulterior aprobación.