OCIM

Política de Seguridad de la Información

V.1

01/01/2023

HISTORIAL DE APROBACIONES Y REVISIONES

La Empresa ha aprobado esta Política de Seguridad de la Información y la revisará y actualizará periódicamente, según sea
necesario.

Fecha de entrada en vigor	Versión	Cambios realizados	Firmas
1 de enero de 2023	1.0	Creación de una Política de Seguridad de la Información	Laurent Mathiot, Director General Arnaud Lapière, Director Técnico

OCIM

Índice

I. Introducción 4
II. Propósito 4
II.A. Excepciones 5
III. Ámbito de aplicación 5
IV. Definiciones 5
V. Funciones y responsabilidades 6
VI. Política de Identificación y Clasificación de Datos 6
VII. Política de Datos del Cliente 7
VIII. Política de Protección de Activos de Información 8
IX. Política de Gestión de Hardware 9
X. Política de Gestión de Redes y Servicios 9
XI. Política de Instalación de Software y Gestión de Conexiones de Hardware 10
XII. Política de Protección de Cuentas 10
XIII. Política de Uso Aceptable 12
XIV. Política de Respuesta a Incidentes 13
XV. Política de Supervisión, Pruebas Periódicas y Revisión de Riesgos 14
XVI. Política de Formación, Aplicación, Medidas Correctoras 15

LM AL

bOXSIGN 4PZX277R-1VPP66YJ

OCIM

I. INTRODUCCIÓN

OCIM Finance («OCIM») es un grupo privado de empresas con sede en París, propiedad de la familia Mathiot y financiado por ella. Los intereses iniciales de la familia en el sector inmobiliario se han diversificado desde entonces en otras actividades, entre las que figuran la financiación y el comercio de metales preciosos y estratégicos a través de OCIM. La expansión de las actividades financieras del Grupo también ha impulsado una expansión geográfica, con una filial en Ginebra.

OCIM funciona como sociedad holding del grupo; OCIM Metals & Mining SA («OMM») y Electrum SA («Electrum») son dos de las principales filiales del grupo. OMM es una empresa financiera y de comercio de metales centrada en el oro, la plata y el platino, con presencia en París y Ginebra, mientras que Electrum proporciona una capacidad de comercio exclusiva para apoyar las actividades del grupo, principalmente con fines de cobertura y gestión de riesgos, con equipos en París y Ginebra.

II. PROPÓSITO

OCIM, sus afiliados y entidades relacionadas (en lo sucesivo «OCIM» o «la Empresa») se comprometen a alcanzar los más altos estándares de profesionalidad y conducta ética en sus operaciones y servicios. Asimismo, espera que sus Representantes (directivos, empleados y terceros conexos, entre otros) lleven a cabo sus actividades empresariales de acuerdo con los más altos estándares éticos de conducta y cumplan todas las leyes aplicables.

La presente Política de Seguridad de la Información (la «Política») tiene por objeto aumentar la concienciación sobre las cuestiones relativas a la seguridad de la información y establecer normas para gestionar, regir y hacer cumplir el programa de gestión de la seguridad de la información. Esta Política pretende complementar, pero no sustituir, cualquier ley aplicable que rija los requisitos de seguridad de la información aplicables a la Empresa y sus filiales.

El propósito de esta Política es establecer los principios subyacentes, el marco y el razonamiento para las prácticas de seguridad de la información de OCIM.

El marco de la Política de Seguridad de la Información de OCIM define las medidas de control básicas que se espera que todas las personas que forman parte de OCIM conozcan y sigan de forma coherente. El objetivo del marco de seguridad y sus políticas conexas es definir unos niveles mínimos de seguridad aceptables para la Empresa y aplicarlos de forma coherente en toda la Empresa.

El nivel mínimo se establece para prevenir la mayoría de los riesgos de seguridad previstos, a la vez que ofrece a la Empresa y a sus filiales la posibilidad de personalizar las normas y los procedimientos locales para satisfacer sus necesidades de seguridad cotidianas.

Además, la Política se establece para prevenir la mayoría de los riesgos previstos en función de las operaciones y el tamaño actuales de la empresa. Por lo tanto, la Política debe actualizarse periódicamente a medida que la empresa modifica sus actividades y su tamaño. Cualquier cambio sustancial en el tamaño, el alcance, las actividades empresariales, las operaciones o los activos de información de la Empresa debe poner en marcha una revisión y actualización de esta Política. Además, debe mantenerse un registro de versiones y un historial adecuado, al igual que con las normas, a fin de mantener la coherencia con los avances tecnológicos. Este registro se mantendrá en el depósito con todas las demás políticas y actividades de mantenimiento de registros de OCIM conexas.

bOXSIGN 4FZX277R-1VPP66YJ

II.A. EXCEPCIONES

Las solicitudes de excepciones a los requisitos de esta Política o a la propia Política deben presentarse por escrito formalmente al Director de Tecnología («CTO») para su revisión. La solicitud de excepción **debe** incluir:

- El motivo comercial por el que se realiza la solicitud; y
- El requisito o apartado específico de la Política que se solicita modificar o del que se solicita una excepción.

El Director de Tecnología se pondrá en contacto con las partes interesadas pertinentes, incluidos, entre otras, las partes interesadas en el ámbito jurídico y de riesgos, para determinar si se requiere una revisión y evaluación adicionales.

Las excepciones tienen una duración razonable, que refleja la necesidad de la empresa y el nivel de riesgo implicado. Si la excepción tiene una vigencia superior a un (1) año, deberá considerarse la posibilidad de actualizar y/o modificar las políticas y procedimientos.

Al vencimiento de una excepción, debe revisarse el riesgo, y el CTO o el Departamento/Asesor jurídico determinarán una prórroga o nuevas medidas.

III. ÁMBITO DE APLICACIÓN

Esta Política es aplicable a los empleados, directivos, gerentes, directores, altos ejecutivos, empleados temporales, contratistas, consultores, temporales, y cualquier otro trabajador, de OCIM, así como a cualquier proveedor y terceros que creen, reciban, almacenen, usen, encuentren o transmitan Información de OCIM. Esta Política abarca la información que se almacena o comparte por cualquier medio, incluida la información electrónica y en papel, y la información compartida oral o visualmente (por ejemplo a través de teléfono y videoconferencias). A efectos de este documento, el ámbito de aplicación de los componentes de infraestructura se limita a la infraestructura de OCIM necesaria para dar soporte a la actividad empresarial.

IV. DEFINICIONES

Una **«política»** es un curso o método de acción obligatorio y definitivo seleccionado por la alta dirección para orientar y determinar las decisiones presentes y futuras. La política es independiente de tecnologías o soluciones específicas. Los expertos en seguridad, cumplimiento de normativas y tecnologías específicas actualizan todas las políticas, como mínimo, una vez al año.

Una «**práctica**» es un mecanismo para llevar a cabo la dirección en materia de políticas de la alta dirección. Las prácticas harán referencia a las normas y procedimientos necesarios utilizados al aplicar una política.

Una «**norma**» es un conjunto de requisitos obligatorios y específicos para satisfacer los objetivos de alto nivel definidos en una política. OCIM debe identificar las prácticas comunes de la industria aplicables a su actividad empresarial y filiales. Asimismo, debe adaptar los controles de seguridad a esos requisitos o utilizarlos como marco base para las normas, seguido de una personalización para cumplir los requisitos

bOXSIGN 4FZX277R-1VPP66YJ

de la política de la organización. En raras ocasiones, los departamentos pueden solicitar excepciones a las normas siempre que sigan un procedimiento de excepción formal.

Un «**procedimiento**» es un conjunto de instrucciones específicas y sistemáticas que describen cómo cumplir los requisitos descritos en una norma o directriz. Estos documentos cambian con frecuencia en función de la tecnología y/o del equipo/persona que realiza la tarea.

Una «**directriz**» es un conjunto de recomendaciones opcionales que apoyan una norma específica. OCIM revisa las directrices en función de las necesidades.

Un «**acuerdo legal**» o «**contrato**» se refiere a todos y cada uno de los instrumentos escritos, acuerdos, documentos, ejecución de escrituras, poderes, transferencias, cesiones, contratos, obligaciones, certificados y otros instrumentosde cualquier naturaleza celebrados por OCIM (por ejemplo, MSA, NDA, SOW).

Este documento delimita las facultades. Cada facultad se caracteriza por una de las siguientes palabras:

- «**deberá**» o «**debe**» indica una actividad o función que el rol está obligado a realizar y no puede rechazar o delegar.
- «**debería**» indica una actividad o función de la que el rol es responsable, aunque su desempeño específico pueda delegarse.
- «**puede**» indica una actividad o función que el rol es capaz de realizar entre sus otras tareas.

V. FUNCIONES Y RESPONSABILIDADES

OCIM utilizará las siguientes clasificaciones para las personas que utilicen los activos digitales de OCIM:

Usuario: cualquier persona que utilice los activos de información de OCIM para fines empresariales legítimos, incluidos terceros externos, como proveedores y contratistas. El Usuario está obligado a cumplir los requisitos establecidos en esta Política. Todos los Usuarios están obligados a informar de los casos de incumplimiento de esta Política. Todo Usuario debe mantener la confidencialidad de los activos de información aunque fallen o no existan mecanismos técnicos de seguridad.

Responsable de TI: cualquier persona(s) explícitamente asignada(s) como responsable(s) del mantenimiento de las operaciones y la seguridad de los activos de información de OCIM. El Responsable de TI, o la persona en quien este delegue, debe garantizar el cumplimiento de los requisitos establecidos en esta Política. El Responsable de TI debe informar a la Dirección de cualquier infracción de esta Política y adoptar medidas correctoras. Las medidas correctoras deben adoptarse en un plazo razonable en función del riesgo y de acuerdo con la Dirección.

Dirección: cualquier persona(s) explícitamente asignada(s) como responsable(s) de las operaciones y del deber fiduciario de OCIM. La Dirección debe supervisar y dirigir el programa de seguridad de la información y aprobar esta Política.

Visitante/Invitado: cualquier individuo(s) que requiera acceso temporal a los activos de información de OCIM para fines limitados o no empresariales (por ejemplo, acceso invitado a Wi-Fi o a impresoras). Los Visitantes y/o Invitados no tendrán acceso a ninguna información contemplada en la Política de Identificación y Clasificación de Datos. El Responsable de TI configurará los activos de información de tal manera que los Visitantes y/o Invitados no puedan acceder a ninguna información interna de OCIM (por

ejemplo, segmentación de sistemas, redes exclusivas para invitados, etc.). Los Visitantes y/o Invitados no recibirán cuentas de usuario de OCIM.

VI. POLÍTICA DE IDENTIFICACIÓN Y CLASIFICACIÓN DE DATOS

La Política de Identificación y Clasificación de Datos define los objetivos de OCIM a la hora de establecer normas específicas para identificar, clasificar y etiquetar los activos de información de OCIM. Esta Política proporciona una práctica para proteger los datos esenciales para la organización y todos los empleados deben ser conscientes de estas clasificaciones y procedimientos de tratamiento.

La clasificación de los datos se basará en su carácter sensible, crítico y su valor. Los datos deben clasificarse en uno de los cuatro (4) niveles: Restringidos/Exclusivos, Confidenciales, Sensibles o Públicos. Todos los datos requieren algún nivel de protección, pero a medida que aumentan su carácter sensible, crítico y su valor también deben hacerlo los controles de seguridad. Los controles de seguridad deben aplicarse de forma proporcional al valor de los datos, su sensibilidad, el riesgo y de acuerdo con los requisitos legales y reglamentarios.

Nivel I: Datos Restringidos/Exclusivos

Información de carácter estratégico, exclusivo o de misión crítica. La pérdida o el daño de esta información probablemente tendría una repercusión adversa **grave o catastrófica** en la capacidad de la organización para continuar sus operaciones, una repercusión adversa **grave o catastrófica** en la reputación de la organización, una repercusión adversa **grave o catastrófica** en el personal o los activos de la organización. Estos datos están destinados a su uso dentro de la organización y a quienes tengan una necesidad empresarial legítima de ellos. Cualquier divulgación externa intencionada de esta información para uso empresarial legítimo (por ejemplo, reguladores, inversores estratégicos, asesores externos, etc.) debe ser coordinada por los Departamentos Jurídico y de Riesgos.

Nivel II: Datos Confidenciales

Información cuyo acceso no autorizado, cesión o destrucción podría causar **graves** daños a OCIM, sus clientes o empleados (por ejemplo, números de identificación, fechas de nacimiento, información sanitaria, información financiera, etc., o colectivamente, «información de identificación personal» o «información personal»). Estos datos están destinados a ser utilizados dentro de la organización y por aquellas personas (internas o externas) que tengan una necesidad empresarial legítima de ellos.

Nivel III: Datos Sensibles

Información que debe protegerse por motivos éticos o de privacidad. El uso, el acceso, la divulgación, la adquisición, la modificación, la pérdida o la eliminación no autorizados de información a este nivel podría causar pérdidas financieras, daños a la reputación de OCIM o violar los derechos de privacidad de una persona. Esto incluye la información confinada para su uso exclusivo con fines relacionados con su actividad.

Nivel IV: Datos Públicos

La información pública es aquella que no se difunde públicamente, pero que puede ser evaluada por el público en general mediante su divulgación legítima. Este tipo de información se define explícitamente como información pública, destinada a ser fácilmente accesible a las personas, o no se clasifica

específicamente en ninguna otra parte de la norma de clasificación de datos protegidos. El conocimiento de información pública no expone a OCIM, sus activos o su personal a daños financieros, de reputación o de otro tipo.

VII. POLÍTICA DE DATOS DEL CLIENTE

Conservación de Datos del Cliente

Para garantizar un tratamiento justo, los Datos del Cliente no serán conservados por OCIM durante más tiempo del necesario en relación con los fines para los que fueron recogidos originalmente, o para los que fueron tratados posteriormente. El periodo de tiempo durante el cual OCIM necesita conservar los Datos del Cliente debe estar recogido en los requisitos legales y contractuales, siempre que sea posible. En ausencia de un requisito legal, reglamentario y contractual, OCIM retendrá los Datos del Cliente basándose en un estándar de mejores prácticas de la industria publicado **y aplicable a la actividad empresarial de OCIM**. Todos los Datos del Cliente deben borrarse o destruirse lo antes posible cuando se haya confirmado que ya no es necesario conservarlos.

Protección de Datos del Cliente

OCIM adoptará medidas físicas, técnicas y organizativas para garantizar la seguridad de los Datos del Cliente, incluyendo, entre otros, la información de identificación personal. Esto incluye la prevención de pérdidas o

daños, alteración, acceso o tratamiento no autorizados, así como otros riesgos a los que puedan estar expuestos en virtud de la acción humana o del medio físico o natural.

El conjunto mínimo de medidas de seguridad adoptadas tiene por objeto:

- Impedir que personas no autorizadas accedan a los sistemas de tratamiento de datos en los que se tratan los Datos del Cliente.
- Impedir que las personas autorizadas a utilizar un sistema de tratamiento de datos accedan a los Datos del Cliente más allá de sus necesidades y autorizaciones.
- Garantizar que los Datos del Cliente durante la transmisión electrónica no puedan ser leídos, copiados, modificados o eliminados sin autorización.
- Garantizar la existencia de registros de acceso para determinar si los Datos del Cliente se han introducido, modificado o eliminado de un sistema de tratamiento de datos, y quién lo ha hecho.
- Garantizar que, en el caso de que el tratamiento lo lleve a cabo un Encargado del Tratamiento (por ejemplo, un tercero distinto de OCIM), los datos solo puedan tratarse de conformidad con la Política de Seguridad de la Información de OCIM.
- Garantizar que los Datos del Cliente estén protegidos contra la destrucción, la pérdida o la corrupción no deseadas.
- Garantizar que los Datos del Cliente recopilados para distintos fines puedan tratarse y se traten de forma independiente, en función de las necesidades y requisitos empresariales.
- Garantizar que los Datos del Cliente no se conserven más tiempo del necesario.

VIII. POLÍTICA DE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

La Política de Protección de Activos de Información define los objetivos de OCIM para establecer prácticas que protejan la confidencialidad, la integridad y la disponibilidad de los activos de información de OCIM.

La Política define los objetivos para gestionar adecuadamente la infraestructura de tecnología de la información de OCIM, incluidas las redes, los sistemas y las aplicaciones que almacenan, procesan y transmiten activos de información. Para esta Política, los activos pueden incluir, entre otros, los siguientes tipos:

- Endpoints (p. ej., dispositivos informáticos aprovisionados y gestionados por OCIM que incluyen, entre otros, ordenadores portátiles, teléfonos inteligentes, tabletas, servidores y equipos de red).
- Dispositivos BYOD (por ejemplo, dispositivos que no son propiedad de OCIM pero que se utilizan para la actividad empresarial de OCIM).
- Datos e información (por ejemplo, código fuente, planes del proyecto, disponibilidad del proveedor del cliente).
- Cuentas de sistema (por ejemplo, cuentas de administrador de ProtonMail, AWS Console, AWS Linux, cuentas de servicio).
- Cuentas de aplicaciones (por ejemplo, HRIS, Confluence, GitHub).
- Software (por ejemplo, Slack, GSuite).
- Cuentas en redes sociales (por ejemplo, cuenta de Twitter de OCIM, Facebook, Instagram, etc.).
- Redes privadas (por ejemplo, activos utilizados para pruebas de desarrollo).
- Conexiones de redes públicas a redes privadas de OCIM (por ejemplo, VPN).
- Instalaciones de oficina.

El nivel mínimo de acceso requerido para satisfacer una necesidad empresarial aprobada se concederá a los recursos de OCIM una vez obtenida la debida aprobación del Responsable de TI y de la Dirección, o de sus delegados asignados. El acceso se concede mediante el establecimiento de cuentas de usuario de acuerdo con el proceso de solicitud de cuentas, y es aprobado por la Dirección de OCIM.

El procedimiento para conceder, revisar y eliminar el acceso debe incluir pruebas de todas las transacciones de provisión y estar disponible para auditorías o revisiones periódicas. El procedimiento para conceder o retirar el acceso debe incluir un dispositivo o mecanismo de seguimiento de la aprobación expresa de la transacción, ya sea en formato electrónico o impreso. Algunos ejemplos son, entre otros, el correo electrónico, las entradas en un sistema de tickets, los formularios firmados y escaneados en formato electrónico, los registros u otros elementos que puedan demostrar que se concedió la autorización adecuada para proporcionar acceso al usuario.

El acceso a los activos de información se limitará a las personas autorizadas cuyas responsabilidades laborales lo requieran, según determine un proceso de aprobación adecuado, y a aquellas autorizadas a tener acceso por requisito legal o reglamentario.

IX. POLÍTICA DE GESTIÓN DE HARDWARE

A medida que cambien el tamaño, el alcance y las operaciones de OCIM, el Responsable de TI, junto con los Departamentos Jurídico y de Riesgos, determinará los casos de uso de hardware adecuados para OCIM.

Dispositivos corporativos

Todos los usuarios de OCIM solo pueden adquirir y registrar dispositivos aprobados por el Responsable de TI. El Responsable de TI, o su delegado, configurará el dispositivo para que cumpla las normas mínimas de OCIM, incluidos, entre otros, el tipo de acceso (p. ej., Active Directory frente a acceso local), los derechos

de control de acceso y grupo (p. ej., usuario normal, privilegios elevados, administrador, etc.) y el software de supervisión y escaneado.

Dispositivos BYOD

OCIM permite, pero desaconseja, el uso de dispositivos personales con fines profesionales. Los usuarios de dispositivos personales:

- Deben aceptar la responsabilidad de cualquier pérdida de datos.
- Deben aceptar el software y los controles de seguridad adicionales que determine el CTO (por ejemplo, software de escaneado, supervisión de la gestión de dispositivos móviles, etc.).
- Solo deben utilizar recursos OCIM SaaS o basados en la nube mediante acceso web.
- No deben instalar el software registrado o propiedad de OCIM en el dispositivo.
- No conectarse o utilizar y compartir archivos en la nube.

X. POLÍTICA DE GESTIÓN DE REDES Y SERVICIOS

A medida que cambien el tamaño, el alcance y las operaciones de OCIM, el CTO, junto con el Departamento Jurídico, determinará los casos de uso apropiados de la red y los servicios para OCIM.

El CTO, o su delegado, se asegurará de que los activos de información estén lógicamente separados y segmentados, para minimizar la exposición al riesgo (por ejemplo, separados por sitio, políticas de grupo, subredes, etc.).

El CTO mantendrá documentación en la que se describa, como mínimo:

- Los servicios en uso.
- Los flujos de datos.
- La ubicación de los datos.

bOXSIGN 4PZX277R-1VPP66YJ

El CTO, o su delegado, establecerá medidas de control (por ejemplo, dispositivos cortafuegos, configuraciones, sistemas de alerta, etc.) para proteger los activos de seguridad de la información.

El CTO puede utilizar una base de datos de gestión de la configuración, o una herramienta similar, para identificar, gestionar y rastrear activos, dispositivos de red y servicios.

XI. POLÍTICA DE GESTIÓN DE LA INSTALACIÓN DE SOFTWARE Y LAS CONEXIONES DE HARDWARE

Todo el software instalado o el hardware conectado a los activos de información de OCIM debe ser evaluado por el CTO antes de su instalación o conexión. La instalación o conexión puede realizarse por indicación del CTO, su delegado o instrucción explícita al usuario. Los usuarios no pueden instalar software ni conectarse al hardware sin permiso. La manipulación de los controles de seguridad para eludir esta Política constituye una infracción.

XII. POLÍTICA DE PROTECCIÓN DE CUENTAS

La Política de Protección de Cuentas define los objetivos de OCIM para establecer prácticas para las cuentas de usuario y su protección.

Características de las cuentas de usuario

Todas las cuentas de usuario de OCIM deben ser únicas y rastreables hasta el usuario asignado. OCIM tomará las medidas adecuadas para proteger la privacidad de la información del usuario asociada a las cuentas de usuario. No se permite el uso de cuentas de grupo ni de contraseñas de grupo, a menos que lo aprueben específicamente el Director Técnico **y** la Dirección, o sus delegados.

Privilegios de la cuenta de usuario

A los usuarios se les concederá el acceso mínimo necesario para realizar sus tareas específicas. La concesión de niveles de acceso a los recursos se basará en el principio del menor privilegio, las responsabilidades laborales y la separación de funciones. El nivel de acceso mínimo requiere la recomendación del responsable del usuario y la evaluación del propietario del sistema de información. El propietario del sistema de información determinará en última instancia el nivel de acceso de un usuario a su sistema.

Cuentas inactivas

Las cuentas se desactivarán después de treinta (30) días de inactividad. Los usuarios que tengan previsto desplazarse a lugares de operaciones sobre el terreno o ausentarse de la oficina durante otros periodos aprobados de ausencia prolongada deberán coordinar su ausencia con el responsable para garantizar la correcta disposición de la cuenta.

Cuentas de usuario temporales

Todas las solicitudes de cuentas de usuario temporales deben indicar una fecha de caducidad que se aplicará en el momento de crear la cuenta. Cuando esto no sea posible, puede utilizarse un mecanismo controlado manualmente. El propietario del sistema supervisará el acceso temporal para garantizar que las actividades se ajusten a la finalidad prevista.

Características de la contraseña

Todas las contraseñas deben construirse utilizando normas de complejidad mínima. Para las mejores prácticas, OCIM puede hacer referencia a normas externas, como *NIST Special Publication 800-63b, Digital Identity Guidelines*, o normas u orientaciones similares conexas.

OCIM puede desplegar una solución de gestión de contraseñas para todos los usuarios con el fin de permitir la rotación regular de contraseñas y la unicidad por servicio.

El CTO configurará los controles para garantizar que se cumplan las normas de complejidad mínima y que se apliquen duraciones de caducidad razonables.

Restablecimiento de contraseña

OCIM establecerá un procedimiento para verificar la identidad de un usuario antes de restablecer su contraseña.

Inicio de sesión automático

No se permitirá el uso de software de inicio de sesión automático para eludir la introducción de contraseñas, salvo con la aprobación específica por escrito del CTO **y** la Dirección, o sus delegados.

Custodia de cuentas de usuario y contraseñas

Cada persona a la que se asigne una cuenta de usuario y una contraseña es responsable de las acciones realizadas con dicha cuenta y no debe divulgar la información de la misma a ninguna otra persona por ningún motivo.

Gestión del acceso a las cuentas de usuario

El acceso de la Dirección a las cuentas de usuario se limitará únicamente a fines empresariales, como durante una situación de emergencia o contingencia, casos de ausencia prolongada del usuario o abuso por parte del usuario de los recursos de información de OCIM.

Transferencias de funciones o responsabilidades

El personal que pase de una función o área de responsabilidad a otra verá modificados sus privilegios de acceso para reflejar sus nuevas responsabilidades laborales.

Cancelación del acceso de usuarios

Dimisión voluntaria. En un plazo de 24 horas, OCIM cancelará el acceso a la cuenta y el acceso físico de los usuarios cuya relación con OCIM haya concluido.

Cese involuntario. OCIM cancelará el acceso a la cuenta y el acceso físico inmediatamente tras la notificación de los Departamentos Jurídico y/o de Recursos Humanos de los usuarios cuya relación con OCIM haya concluido.

El CTO debe coordinar los requisitos de retención de datos y cuentas de usuario con los Departamentos Jurídico y de Recursos Humanos correspondientes antes de purgar, eliminar o

LM AL
bOXSIGN 4PZX277R-1VPP66YJ

modificar datos o información de usuario de un empleado o usuario saliente.

Tiempo de espera de la sesión de usuario

Las sesiones de usuario expirarán después de 20 minutos de inactividad, a menos que se especifique lo contrario como parte del plan de seguridad del sistema o de la aplicación. Esto incluye las conexiones de los usuarios a Internet o a aplicaciones específicas.

Acceso a información sensible

Como parte del compromiso de OCIM con la protección de la Información Sensible, se llevarán a cabo verificaciones de antecedentes para todos los candidatos finales que se consideren para el empleo. Estas personas estarán sujetas a las disposiciones de las políticas y procedimientos de OCIM para proteger y salvaguardar dicha información de la divulgación no autorizada. La comprobación de antecedentes puede incluir, entre otras cosas, la comprobación de antecedentes penales.

XIII. POLÍTICA DE USO ACEPTABLE

Los activos de información de la Empresa no se utilizarán como foro para promover causas religiosas o políticas, ni ninguna actividad ilegal. Asimismo, están prohibidos en los sistemas de la Empresa los mensajes u opiniones ofensivos o inapropiados, la transmisión de imágenes, mensajes, dibujos animados u otros elementos sexualmente explícitos, o los mensajes que puedan interpretarse como acoso o menosprecio de otras personas por motivos de raza, color, edad, nacionalidad, religión, sexo, veteranía, discapacidad o cualquier otra condición protegida por la legislación internacional, federal, estatal, regional y/o local aplicable.

Los empleados son responsables de ejercer el buen juicio en el uso personal de los sistemas de la Empresa. En ausencia de políticas específicas relativas al uso personal de los sistemas de la Empresa, los empleados deben consultar a su supervisor o responsable para obtener orientación.

No se garantiza la privacidad al utilizar la infraestructura de OCIM. La información creada o almacenada en los equipos de OCIM se considera propiedad intelectual de OCIM. La Dirección se reserva el derecho de supervisar la actividad informática y examinar las incidencias de cualquier equipo en cualquier momento.

Herramientas de comunicación y almacenamiento de datos

OCIM recomienda a los usuarios que utilicen únicamente herramientas de comunicación que admitan el cifrado de extremo a extremo y el cifrado de datos en reposo.

El CTO pondrá a disposición de los usuarios una lista de herramientas de comunicación autorizadas. Esta lista se revisará periódicamente.

Los usuarios limitarán el uso de aplicaciones móviles de mensajería y chat para fines empresariales si no se dispone fácilmente de una solución corporativa.

Los datos solo se almacenarán en herramientas aprobadas por el CTO. El CTO pondrá a disposición de los usuarios una lista de soluciones autorizadas de almacenamiento de datos. La solución debe utilizar los métodos y normas de cifrado actuales más razonables.

Los datos se etiquetarán de acuerdo con la Política de Identificación y Clasificación de Datos mientras estén en uso y almacenados.

El acceso a las soluciones de almacenamiento de datos de OCIM por parte de terceros debe reducirse al mínimo y emplear la metodología del «menor privilegio» si existe un uso empresarial legítimo para el acceso externo.

Uso prohibido

La siguiente lista de artículos tiene prohibido su uso o almacenamiento en los activos de OCIM:

bOXSIGN 4FZX277R-1VPP66YJ

bOXSIGN 4FZX277R-1VPP66YJ

- Uso de cualquier unidad USB o medios de extracción similares (por ejemplo, discos duros, dispositivos de almacenamiento inalámbricos, etc.) para descargar o cargar cualquier información o contenido desde o hacia cualquier activo de OCIM.
- Artículos que puedan constituir una violación de los derechos de autor, secretos comerciales, patentes u otras leyes o reglamentos de propiedad intelectual, incluyendo, pero no limitándose a, la instalación o distribución de productos de software «pirateados» o de otro tipo que no tengan la debida licencia para su uso por parte de OCIM.
- Exportar software, información técnica, software de encriptación o tecnología, infringiendo las leyes internacionales o regionales de control de exportaciones.
- Introducir software malicioso en la red, o en cualquier otra forma que pueda interferir, dañar o dificultar la seguridad o integridad de cualquier activo de OCIM.
- Eludir o evitar los requisitos de la Política de Seguridad de Endpoints en los dispositivos (por ejemplo, jailbreaking, desactivación de funciones, eliminación de la supervisión, etc.).
- Revelar la contraseña de la cuenta a otras personas o permitir el uso de la cuenta a otras personas.
- Dar o prestar un activo de la empresa a otra persona sin el consentimiento escrito de la dirección autorizada.
- Utilizar un activo de la empresa (cualquier dispositivo o host en una red de OCIM) para participar activamente en la obtención o transmisión de material que infrinja las políticas o leyes de OCIM sobre acoso u hostilidad en el lugar de trabajo en la jurisdicción local del usuario.
- Realizar ofertas fraudulentas de productos, artículos o servicios procedentes de cualquier cuenta de la empresa.
- Interrumpir las comunicaciones de red.
- Eludir la autenticación de usuario o la seguridad de cualquier host, red o cuenta.
- Falsificar o suplantar la identidad, incluidos, entre otros, el correo electrónico, las cuentas o la voz.
- Usar servicios de mensajería o redes sociales para tergiversar la imagen de OCIM o violar las políticas empresariales conexas.
- Usar los activos de OCIM para fines o beneficios personales, que no sean usos o beneficios incidentales, o en violación de cualquier acuerdo entre el usuario y OCIM, como el manual del empleado o el acuerdo de no divulgación del empleado.
- Reenviar o usar servicios de mensajería para participar en esquemas ponzi, en cadena o piramidales.
- Reenviar correos electrónicos, documentos, software e información interna y exclusiva de OCIM a cuentas de correo electrónico personales.

XIV. POLÍTICA DE RESPUESTA A INCIDENTES

OCIM llevará a cabo actividades de respuesta a incidentes de acuerdo con el Plan de Respuesta a Incidentes («IRP», por sus siglas en inglés). El IRP será desarrollado y gestionado conjuntamente por el Responsable de TI, el Departamento Jurídico y el Departamento de Riesgos. El IRP deberá:

- Describir la estructura y la organización de la capacidad de respuesta a incidentes de OCIM.
- Identificar las funciones y responsabilidades de las partes interesadas internas y externas.
- Ajustarse a los requisitos específicos de la organización, incluidos, entre otros, la tolerancia al riesgo, la misión, la visión, la estrategia y las operaciones.
- Definir los incidentes denunciables, incluidos, entre otros, pruebas de acceso no autorizado, pruebas de filtración de datos, pruebas de malware o código malicioso, pruebas de ataques o interrupciones del servicio, pruebas de patrones de ataque sostenidos.
- Definir los recursos y las necesidades de apoyo a la gestión para gestionar y mantener eficazmente el programa de respuesta a incidentes y los incidentes activos.

LM AL
bOXSIGN 4PZX277R-1VPP66YJ

- Definir los requisitos técnicos para gestionar y mantener eficazmente el programa de respuesta a incidentes y los incidentes activos.
- Identificar las actividades de planificación de contingencias y los recursos necesarios en caso de incidente.

- Incluir índices de criticidad para ayudar a los responsables de la respuesta y a los evaluadores a determinar el ámbito de aplicación y la repercusión.
- Incluir un método para documentar y archivar adecuadamente los incidentes del sistema con pruebas de auditoría apropiadas. Ajustar la duración del almacenamiento a la política de conservación de documentos establecida.
- Actualizarse periódicamente para adaptarse a los cambios de la organización.
- Contar con la aprobación de la Dirección.

XV. POLÍTICA DE SUPERVISIÓN, PRUEBAS PERIÓDICAS Y REVISIÓN DE RIESGOS

Para proteger mejor sus activos de información de manera continua, OCIM instituirá capacidades razonables y apropiadas de evaluación y supervisión de amenazas en toda su infraestructura y dispositivos. Además, OCIM realizará pruebas periódicas de sus activos de información y revisará regularmente su postura ante los riesgos de seguridad de la información.

Evaluación y control de amenazas

OCIM identificará, analizará y priorizará periódicamente las amenazas a los activos de información, e integrará los resultados de las actividades de evaluación de amenazas, según corresponda, en la mejora de la postura de seguridad de los activos de información de OCIM.

Basándose en la razonabilidad, las amenazas y las tolerancias de riesgo, OCIM llevará a cabo una supervisión de detección de intrusiones en tiempo real y un análisis periódico de detección de intrusiones para detectar amenazas y actividades de intrusión en segmentos críticos de la red basándose en los resultados del análisis de amenazas.

Evaluación y gestión de la vulnerabilidad

A medida que cambien el tamaño, el ámbito de aplicación y las operaciones de OCIM, el Director de TI, junto con los Departamentos Jurídico y de Riesgos, determinará las medidas adecuadas para llevar a cabo evaluaciones de vulnerabilidad. Como mínimo, OCIM realizará escaneos trimestrales de los activos de información de OCIM para identificar vulnerabilidades, o en algún otro intervalo regular apropiado al tamaño, el ámbito de aplicación y las operaciones actuales de OCIM.

Como mínimo, OCIM realizará anualmente una prueba de penetración externa de su red y de los activos pertinentes.

Se establecerá un proceso formal para identificar, rastrear, reparar o mitigar las vulnerabilidades técnicas utilizando los hallazgos identificados a partir del escaneo de vulnerabilidades, las pruebas de penetración, la respuesta a incidentes y las actividades de evaluación de riesgos. Para apoyar estas actividades, OCIM establecerá un procedimiento o programa formalizado de gestión de parches.

En los casos en que OCIM no pueda realizar un escaneo o prueba en el sistema (por ejemplo, gestionado por un tercero), OCIM buscará algún tipo de atestación, validación o certificación por parte del responsable de que

bOXSIGN 4PZX277R-1VPP66YJ

su entorno es escaneado regularmente en busca de vulnerabilidades; que las vulnerabilidades son remediadas, y que existe algún tipo de programa formal de gestión de parches.

Gestión de riesgos

Las evaluaciones de riesgos para la seguridad de la información deben identificar, cuantificar y priorizar los riesgos en función de criterios de aceptación de riesgos y objetivos pertinentes para OCIM. Los resultados deben orientar y determinar las medidas y prioridades de gestión adecuadas para gestionar los riesgos de seguridad de la información y aplicar los controles seleccionados para proteger contra estos riesgos.

Las evaluaciones de riesgos para la seguridad de la información deben incluir el enfoque sistemático de estimar la magnitud de los riesgos (análisis de riesgos) y el proceso de comparar los riesgos estimados con los criterios de riesgo para determinar su importancia (evaluación de riesgos).

Las evaluaciones de los riesgos para la seguridad de la información deben realizarse de forma metódica y capaz de producir resultados comparables y reproducibles. Las evaluaciones de riesgos para la seguridad de la información deben tener un ámbito de aplicación claramente definido para ser eficaces y deben incluir relaciones con evaluaciones de riesgos en otras áreas, si procede.

Como mínimo, OCIM llevará a cabo una evaluación anual de los riesgos para la seguridad de la información.

XVI. POLÍTICA DE FORMACIÓN, APLICACIÓN, MEDIDAS CORRECTORAS

A medida que cambien el tamaño, el ámbito de aplicación y las operaciones de OCIM, el Responsable de TI, junto con los Departamentos Jurídico y de Riesgos, determinará las actividades y los requisitos adecuados en materia de formación, cumplimiento y medidas correctivas.

Formación

Todos los usuarios a los que asista OCIM revisarán y reconocerán esta Política de Seguridad de la Información y las políticas, normas y directrices pertinentes. Tras su actualización y revisión periódicas, OCIM comunicará los cambios a los usuarios.

Todos los usuarios tendrán acceso a la Política de Seguridad de la Información y a las políticas, normas y directrices pertinentes a través de la solución de almacenamiento compartido de datos de OCIM.

Todos los usuarios deberán certificar que han leído y comprendido las políticas con carácter anual y como parte del proceso de incorporación.

En el momento de la contratación, todos los nuevos usuarios o las nuevas contrataciones deben recibir la educación y la formación adecuadas en materia de seguridad. Una vez finalizada la formación, los nuevos usuarios de OCIM y las nuevas contrataciones deberán firmar que han completado la formación.

OCIM mantendrá un registro de la finalización y el reconocimiento de la formación sobre concienciación en materia de seguridad.

Aplicación

El incumplimiento de cualquiera de las políticas, normas, directrices y procedimientos del Programa de Seguridad de la Información de OCIM puede dar lugar a medidas disciplinarias que pueden incluir el

LM AL
bOXSIGN 4PZX277R-1VPP66YJ

despido de los empleados o la rescisión de los contratos de contratistas, socios, consultores y otras entidades. OCIM también se reserva el derecho de emprender acciones legales en casos que impliquen infracciones de los reglamentos y leyes aplicables.

Medidas correctivas

Cualquier usuario de OCIM que identifique una infracción de las Políticas de Seguridad de la Información de OCIM está obligado a reportar la infracción de inmediato a su responsable, al CTO o a Recursos Humanos. Al aplicar medidas correctivas, la Dirección o RR. HH. seguirán las políticas pertinentes de OCIM.

LM AL
bOXSIGN 4PZX277R-1VPP66YJ

ANEXO A: PÁGINA DE FIRMAS

OCIM

RECEPCIÓN Y ACUSE DE RECIBO

Por la presente, reconozco que he recibido, leído detenidamente y comprendido la «Política de Seguridad de la Información» de OCIM y acepto cumplir en todos los aspectos con todos los procedimientos a los que estoy sujeto/a.

Entiendo que el Director General está disponible para responder a cualquier pregunta que tenga en relación con la Política de Seguridad de la Información del Grupo OCIM.

5nov 2024

bOXSIGN 4PZX277R-1VPP66YJ

Firma

Fecha

Laurent Mathiot

Nombre (en letra de imprenta)

bOXSIGN 19Z23P84-1VPP66YJ

Firma

5 nov. 2024

Fecha

Arnaud Lapiere

Nombre (en letra de imprenta)