Contenido de Seguridad de la Información para OCP.

¿Qué es OCP?
La OCP es la nueva plataforma de declaraciones en línea de reclamos. Conecta digitalmente a proveedores y clientes certificados FSC® de modo que las declaraciones de productos certificados FSC puedan ser rápidamente confirmadas como exactas por ambas partes comerciales. A medida que los productos se desplazan por la cadena de suministro, su certificación FSC puede ser garantizada. Este sistema mejorará la integridad de la marca FSC.

FSC prevé que el uso de la OCP podría reducir significativamente la carga administrativa de la certificación FSC. Por lo tanto, estamos identificando las posibles formas en que partes más grandes del estándar de CdC puedan ser cumplidas de forma automática por las organizaciones certificadas que integran completamente a la OCP. Estos cambios podrían conducir a un ahorro de tiempo en los procesos de administración y auditoría, de la mano de la construcción de un sistema FSC más robusto.

Si desea obtener más detalles, por favor visite ocp-info.fsc.org.

¿Que información recopila la OCP?

OCP tendrá la información del certificado de su organización, la cual esta disponible públicamente en info.fsc.org.

Los usuarios de OCP pueden localizar y conectarse a sus proveedores o clientes y registrar información de productos certificados FSC comercializados entre las partes.

La información introducida sobre los bienes comercializados se limita al identificador de transacción, fecha, tipo de declaración, tipo de producto, volumen comercializado, descripción y especies en caso corresponda.

OCP no recoge ninguna información financiera o de propiedad.

Si desea más detalles puede acceder al Sitio de Ayuda OCP, específicamente, Campos de información en la OCP.

¿Cómo mantenemos segura la información de la OCP?
Estamos comprometido a proteger los activos de información que guardamos para nuestros clientes, socios, así como nuestros propios activos de información por lo que hemos establecido objetivos para la gestión de seguridad de la información. Esto incluye la certificación ISO 27001 Q3 2014. ISO 27001 es un estándar de seguridad reconocido mundialmente el cual proporciona lineamientos para las políticas y controles que una organización tiene en marcha para resguardar la información. El estándar establece requisitos convenidos internacionalmente y mejores prácticas para el enfoque sistemático del desarrollo, despliegue y administración del sistema de gestión de seguridad de la información basado en riesgos / amenazas.

Lo que esto significa en la práctica es:
HF opera y mantiene un sistema de gestión de seguridad de la información (SGSI) para controlar sus activos de información adecuadamente. Esto incluye la clasificación de todos los activos con directrices claras sobre cómo la información puede ser manejada.

HF ha implementado y aplica las políticas internas y procedimientos que respaldan el SGSI. Como parte de un sistema de gestión es auditado de forma independiente por Certification Europe, por lo menos anualmente y por especialistas en seguridad para garantizar el cumplimiento de los requisitos.

La capacitación en temas de seguridad es parte de nuestra inducción y procesos continuos de desarrollo del personal, garantizando que nuestro equipo sea consciente de las políticas y procedimientos para salvaguardar la seguridad de la información.

Nosotros implementamos controles de seguridad humanos, organizacionales y tecnológicos, impulsados por los controles del SGSI (Declaración de aplicabilidad) para proteger los activos de información contra el acceso no autorizado, fugas, modificación, robo / pérdida, ataques de denegación de servicio, o cualquier otra amenaza.

Tomamos las infracciones con seriedad y tenemos un proceso formal de gestión de incidentes para identificar, contener y recuperarse de un incidente de seguridad si es que este llegara a darse, con gran predisposición para informar a nuestros usuarios.

HF a través de su SGSI hace esfuerzos para localizar rápidamente la causa principal, mantener el daño a un mínimo y prevenir las recurrencia si ocurre un incidente que representa una amenaza para los activos de información.

HF cumple con todos los requisitos legales / regulatorios y contractuales relacionados con la seguridad de la información y adopta las directrices de las leyes del Reino Unido, estándares de la industria y buenas prácticas para seguridad de la información.

HF revisa y mejora continuamente estas actividades a través de auditorías internas, el ejercicio y la revisión de nuestros procedimientos.

En línea con nuestros controles SGSI de detección y resolución de fallos de seguridad incluyen el uso de pruebas de penetración de seguridad periódicas de la OCP, las cuales son llevadas a cabo por un tercero independiente, el Grupo NCC.

HF presta sus servicios en base al siguiente marco legal / regulatorio

- Ley de Telecomunicaciones.
- Ley de Protección de la Información
- Contratos con los clientes de Historic Futures.
- HF utiliza asesores legales externos para consejería.

Si desea más detalles, puede revisar el ISO27100.

¿Qué sucede si algo sale mal?

Tomamos las infracciones con seriedad y tenemos un proceso formal de gestión de incidentes para identificar, contener y recuperarse de un incidente de seguridad si es que este llegara a darse, con gran predisposición para informar a nuestros usuarios.

HF a través de su SGSI hace esfuerzos para localizar rápidamente la causa principal, mantener el daño a un mínimo y prevenir las recurrencia si ocurre un incidente que representa una amenaza para los activos de información.

Todos los incidentes se clasifican dependiendo de su severidad de acuerdo con nuestro procedimiento de gestión de riesgos SGSI. Todos los incidentes con una magnitud de Prioridad 2 o superior se publicarán en ocp-status.fsc.org un sitio web público e independiente. (Actualmente alojado en http://ocpstatus.tumblr.com/) Los usuarios OCP también tendrán acceso a nuestro sistema de tickets que permite a los usuarios reportar cualquier problema o incidente que pueda surgir.

A continuación se presentan algunas de las preguntas más frecuentes formuladas por nuestros usuarios. Si algún usuario advierte algo sospechoso, por favor póngase en contacto con nosotros a través de nuestro servicio de soporte haciendo clic aquí.

ESTÁNDARES Y CONTROLES

¿Qué estándares y controles de seguridad están en marcha?

La administración de HF se compromete a proteger los activos de información que mantiene para nuestros clientes, socios, así como nuestros propios activos de información y ha establecido objetivos para la gestión de seguridad de la información. Esto incluye la certificación ISO 27001 que es el estándar de seguridad reconocido a nivel mundial que proporciona una guía de las políticas y controles que una organización debe disponer para asegurar su información. El estándar establece requisitos acordados internacionalmente y las buenas prácticas para el enfoque sistemático del desarrollo, despliegue y gestión del sistema de gestión de seguridad de la información basado en riesgos / amenazas.

¿Ustedes se adhieren al SAS 70?

HF ha implementado un SGSI al estándar internacional de gestión de seguridad ISO 27001, este estándar tiene un número de ventajas sobre la declaración de seguridad SAS70. El estándar especifica las buenas prácticas de gestión de seguridad y tiene controles de seguridad exhaustivos. La certificación bajo el estándar requiere a HF:

- Evaluar sistemáticamente nuestros riesgos de seguridad de la información, teniendo en cuenta el impacto de las amenazas y vulnerabilidades de la compañía.
- Diseñar e implementar un conjunto completo de controles de seguridad de la información y otras formas de gestión de riesgos para abordar los riesgos de seguridad de la empresa.
- Adoptar un proceso de gestión global para garantizar que los controles de seguridad de la información satisfagan nuestras necesidades de seguridad de información de manera permanente.

La clave para la certificación en curso según este estándar es la gestión eficaz de un programa de seguridad riguroso. El requisito SGSI define la forma en que manejamos continuamente la seguridad de manera integral y completa. La certificación ISO 27001 se centra específicamente en el SGSI de HF y mide cómo nuestros procesos internos siguen el estándar ISO. La certificación anual por el tercer auditor independiente acreditado confirma que nuestros procesos y controles están operando alineados con el estándar 27001.

SOC 1 / SSAE 16 / ISAE 3402 (formalmente SAS 70) es un estándar de auditoría utilizado para permitir que un auditor independiente evalúe y proporcione un informe de auditoría sobre los objetivos y las actividades de control de la compañía. A nivel mundial ISO 27001 está siendo utilizado por más compañías para proporcionar la garantía de negocio a medida que requiere una gestión continua y realce de los riesgos y controles a través de un modelo de mejora continua a diferencia de la anterior declaración SAS70.

El compromiso para un SGSI de HF se resume en la siguiente tabla basada en las diferencias entre cada estándar.

Metodología	**ISO 27001**	**SOC 1/SSAE, 16/ISAE 3402**
Uso previsto en Negocios	Requisitos de Gestión	Guía de auditoría para los requisitos mínimos
Garantía	Certificación internacional	Reporte de los auditores de servicio
Alcance	Enfoque de negocios para una y todas las formas de información y / o sistemas	Enfoque Financiero (declaraciones y sistemas relacionados)
Postura	Proactiva	Reactiva
Riesgo	Identificar, medir y remediar	Maximizar el riesgo y luego reducirlo
Control de Definición y Medición	Cada control se define y se mide como un requisito de un SGSI	El informe de auditoría Tipo 1 proporciona hallazgos pero no cubre la prueba o eficacia de los controles. La prueba de los controles se incluye en el informe de auditoría de Tipo III.
Mejora Continua	Actualizaciones obligatorias con “plan-do-check-act”	No se incluye

¿Qué políticas de seguridad, estándares se aplican?

HF ha desarrollado políticas y procedimientos basados en las buenas prácticas de la industria y vendedores para proteger los activos de información que mantiene para nuestros clientes, socios y nuestros propios activos de información. La gestión de las comunicaciones y las operaciones está prevista y desplegada con respecto a la seguridad de los activos de información de HF y las operaciones de todo el entorno del procesamiento de la información.

La política y procedimientos establecen estándares para lo siguiente:

• Política de seguridad de la información
• Política de despeje y limpieza del escritorio y pantalla
• Política de eliminación de activos
• Política de cifrado
• Política de control de acceso
• Política de uso aceptable
• Política de computadores móviles
• Política de los servicios de red
• Política de intercambio de información
• Política de continuidad del negocio
• Procedimiento de Gestión de incidentes
• Procedimientos de clasificación de Información
• Procedimiento de gestión de riesgos

Procedimiento de auditoría interna:

• Procedimiento de control de documentos y registros
• Procedimiento de acciones correctivas
• Procedimiento de Acciones preventivas

Cada política y procedimiento respalda los controles requeridos establecidos por la Declaración de Aplicabilidad del estándar ISO 27001 y cómo HF gestiona sus activos de información.

¿Quién audita la política SGSI de HF?
Certification Europe.

HF tiene una carta de certificación de noviembre de 2013, de una consultora de seguridad externa que proporciona nuestra postura de seguridad y compromiso y cumple con el propósito de la ISO 2700 para obtener la certificación.

Se llevó a cabo una revisión externa por parte de una compañía de seguridad externa, CQR en 2013 de acuerdo al ISO 27001 e incluye:

• Documentación del Sistema de Gestión
• Gestión de Riesgos
• Gestión de Documentos y Registros
• Formación, sensibilización y competencia
• Incidentes, Acciones Correctivas y Preventivas
• Planificación de la Continuidad del Negocio
• Implementación de Control

HF completa las pruebas de penetración sobre la eficacia de los controles técnicos.

HF está atravesando un proceso de configuración para obtener la certificación por un organismo independiente Certification Europe. La evaluación de certificación consta de dos fases, la Fase 1 está prevista para mayo y es completada in-situ por el auditor para determinar si el sistema de HF ha cumplido con los requisitos del estándar y apto para ser certificado. La Etapa 2 sigue después de la Etapa 1 y es una auditoría de la eficacia del sistema. Ambas etapas deben cumplirse para obtener la certificación. La Etapa 2 está prevista para junio de 2014 y la certificación es obtenida después de este momento.

Cada etapa se completa in situ e incluye:

• Observación de procesos / actividades y personal

• Revisión de documentos, controles y registros

• Conversaciones con la administración del sitio y el personal

El organismo certificador proporciona auditorías de vigilancia continuas cada año, basadas en el muestreo del SGSI de HF para garantizar que HF mantiene la certificación.

¿Quién lleva a cabo las pruebas de penetración de la OCP?
De acuerdo a nuestros controles SGSI se llevan a cabo pruebas periódicas de OCP por un tercero independiente, nuestro actual proveedor de servicio es NCC Secure.

IFORMACION Y ALMACENAMIENTO

¿Dónde se almacena mi información?
La información es alojada en Amazon Web Services en sus centros de datos Europeos con sede en Dublín, Irlanda.

El centro de información es propiedad de Amazon Web Services y es una filial de Amazon.com, Inc. o sus filiales ("Amazon.com"). Las empresas del Grupo Amazon han certificado que se adhieren a los Principios de Privacidad de Puerto Seguro acordados por los EE.UU. y la UE.

Si desea más detalles puede revisar la información de seguridad de Amazon.

¿Han evaluado el riesgo asociado con el almacenamiento externo?
HF utilizó una empresa de seguridad independiente para realizar una evaluación de riesgos para la solución de alojamiento con el objetivo clave de proporcionar a HF un nivel de garantía de que la solución de alojamiento proporciona controles de seguridad eficaces y apropiados para su información y que no se presenta un riesgo a través del uso de procesamiento y almacenamiento externo.

Amazon EC2 cumple con las normas, estándares y buenas prácticas para mantener la seguridad y protección de datos para proporcionar un nivel de garantía de protección. Estos incluyen ISO27001, HIPAA, SOC 1 / SSAE 16 / ISAE 3402 (anteriormente SAS70), SOC 2, 3 SOC, PCI DSS Nivel 1, FedRAMP (SM), DIACAP y FISMA, ITAR, FIPS 140-2, CSA, MPAA.

El sistema se llevará a cabo simultáneamente en dos zonas de disponibilidad Amazon (el equivalente a dos centros de datos diferentes). (Primavera de 2014, sólo un centro de datos actualmente operativo)

CONTROLES DE ACCESO

¿Quién puede acceder a nuestra información OCP?
La información de certificado puede ser accedida por los titulares de la cuenta y administradores de la cuenta, los permisos de usuarios son gestionados por el administrador de la cuenta desde el servicio OCP.

La información de la declaración puede ser vista por ambas partes comercial en el proceso de confirmación de declaraciones.

Los administradores de Amazon AWS no tienen acceso a las instancias de los clientes, y no pueden iniciar sesión en el sistema operativo del invitado.

Historic Futures, soporte FSC y los organismos certificadores no tienen habitualmente el acceso a menos que sea concedido por el administrador de la cuenta.

Si desea más detalles puede revisar los Términos y Condiciones completos.
Como se indica en los Términos y Condiciones: "FSC se reserva el derecho de autorizar a Historic Futures a supervisar, revisar y / o retener en todo momento cualquier actividad derivada de la cuenta de Usuario Autorizado exclusivamente con el fin de garantizar un buen funcionamiento del sistema y / o divulgar cualquier información en la medida que sea necesaria para acatar cualquier ley, reglamento, proceso legal, amenaza de accion legal o pedidos del gobierno oficial aplicables". Por lo tanto, esto significa que si un TC tiene una pregunta / problema con el OCP y necesita compartir cualquier información de cuenta de OCP con el personal de apoyo, es ahí cuando el FSC podría tener acceso a su cuenta- con el único propósito de ayudar al TC CH después de que este TC lo haya solicitado.

¿Cuáles son los controles de seguridad físicos de Amazon?
El acceso físico es controlado estrictamente tanto en el perímetro como en los puntos de ingreso al edificio por parte de personal de seguridad profesional utilizando video vigilancia, los más actuales sistemas de detección de intrusos, y otros medios electrónicos. El personal autorizado debe pasar por una autenticación de dos factores por lo menos tres veces para poder acceder a los centros de datos. Todos los visitantes y contratistas deben presentar identificación y son registrados y escoltados por personal autorizado continuamente.
Gestión de Incidentes

¿Qué procedimientos existen para protegerse contra el acceso no autorizado al sistema y el acceso físico a los centros de datos?
El acceso a los activos de información de HF está en función a las necesidades con el fin de reducir los riesgos asociados con el uso indebido, como alteración, destrucción y divulgación no autorizada de información. La política de seguridad de la información de HF establece líneas de base para la Gestión del Acceso que cubre:

• Registro de usuarios e identificación

Roles y responsabilidades

• Aprobación de acceso por parte del Propietario

• Autenticación de usuario

• Autorización de usuario

• Gestión de privilegios

• Control del Sistema Operativo

• Control de acceso a la red

• Administración de contraseña de usuarios

• Revisión de los derechos de acceso

• Acceso remoto

GESTIÓN DE INCIDENTES Y RECUPERACIÓN DE DESASTRES

¿Cómo están dispuestas la copia de seguridad y restauración en caso de corte de luz, fuego, violación?
Las bases de datos maestras son respaldadas cada hora en Amazon S3. Mantenemos el historial de 10.000 copias de seguridad.

¿La OCP puede intercambiar entre centros de información?
La OCP ha sido diseñada para funcionar a través de múltiples centros de datos, la pérdida de un solo centro de datos no debe resultar en tiempo de inactividad.

¿Cuál es su plan de recuperación de desastres (PRD)?
El sistema OCP se construye a partir de máquinas virtuales genéricas y es diseñado de manera que la pérdida de cualquier máquina no resulte en tiempo de inactividad.

Cada servidor se construye a partir de un estándar y se puede reconstruir, a pedido, en cuestión de minutos.

¿Cómo se controlan los niveles de desempeño?
El servicio independiente provisto por Pingdom.com se utiliza para monitorear el tiempo de actividad del sistema y el tiempo de respuesta desde una serie de lugares en todo el mundo. FSC tiene un acuerdo SLA con Historic Futures que regula los tiempos de respuesta del sistema.

¿Cuál es la meta de desempeño del tiempo de actividad para el servicio OCP?
El tiempo de actividad / disponibilidad SLA acordado es del 99% medido mensualmente.

¿Qué procedimientos existen para protegerse contra virus, códigos maliciosos y software no autorizado?
La política de seguridad de la información de HF establece líneas de base para monitorear mecanismos para identificar las tendencias de seguridad y detectar anomalías. Las anomalías son revisadas para determinar si son indicativas de un evento de seguridad. Los eventos se informan, investigan, intensifican, y corrigen para permitir el rápido retorno a las operaciones normales del negocio. El proceso abarca la detección de eventos y respuesta y la gestión de vulnerabilidades.

¿Qué procedimientos existen para protegerse contra la corrupción del software y la pérdida de datos?
Cuando HF propone nuevos sistemas o cambios a los actuales, se incluyen los aspectos de seguridad de los sistemas de análisis y especificación. Estas especificaciones cubren medidas de seguridad automatizadas y manuales respaldadas por una evaluación de riesgo.

Las líneas de base incluyen:

• Seguridad de los archivos del sistema
• Planificación, aceptación y adquisición de sistemas
• Desarrollo del sistema
• Validación de datos

HF utiliza la planificación de la continuidad del negocio (PCN) para sus recursos empresariales a fin de reducir al mínimo el efecto de un desastre o una interrupción del negocio. La PCN dentro de HF proporciona procedimientos documentados para permitir que el proceso de negocio continúe en caso un activo sea destruido o no esté disponible. La planificación de recuperación de desastres (PRD) es el proceso de recuperar un activo electrónico después que un evento haya hecho que el activo no esté disponible para la empresa.

Las líneas de base para la solidez empresarial incluyen:

• Planificación
• Pruebas
• Mantenimiento
• Sensibilización
• Copia de seguridad y recuperación

¿Cómo puedo reportar un problema de seguridad?
A través de nuestro sistema de tickets: support@ocphelp.zendesk.com

¿Tienen un Oficial de seguridad/ Director de Privacidad designado?

- De acuerdo a los requisitos del SGSI, Historic Futures tiene un propietario de seguridad designado.

En el caso de una crisis, ¿cómo y cuándo el FSC se comunicara conmigo?
Todos los incidentes se clasifican dependiendo de su severidad de acuerdo con nuestro procedimiento de gestión de riesgos SGSI. Todos los incidentes con una magnitud de Prioridad 2 o superior se publicarán en ocp-status.fsc.org un sitio web público e independiente. (Actualmente alojado en http://ocpstatus.tumblr.com/)

¿Seré notificado de todos los problemas e incidentes relacionados con la privacidad (por ejemplo, incumplimiento de privacidad de la información) que involucren y / o impacten a mi información?
HF opera un procedimiento de gestión de incidentes que se lleva a cabo siempre que se produce un incidente de seguridad o privacidad. La respuesta varía apropiadamente con una fuerte inclinación a la comunicación.