Política de seguridad para proveedores

UC - United Capital Puesto de Bolsa, S.A.
Miembro de la Bolsa de Valores de la República Dominicana
SIV-PB-017

Contenido

OBJETIVO

Garantizar la protección de los activos de UC-United Capital Puesto de Bolsa, S.A. (en lo adelante "United Capital") que sean accesibles por los proveedores, así como mantener un nivel apropiado de seguridad de la información y la entrega del servicio acorde con los acuerdos por sus terceras partes.

ALCANCE.

Proveedores de servicios y terceros relacionados que brindan sus servicios en UC- United Capital Puesto de Bolsa.

1. DESARROLLO DE LA POLÍTICA

1.1.1 En las situaciones en que se requiera contratar servicios de resguardo de activos de información, tales como servicios de hosting e infraestructura, plataforma tecnológica, DataCenters y procesamiento, almacenamiento de información física o digital, entre otros, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados, los que deberán tener, a lo menos, el mismo estándar que los existentes en esta Institución.

1.1.2 Los proveedores sólo podrán desarrollar para United Capital aquellas actividades cubiertas bajo contrato de prestación de servicios. De este modo, se entenderá que todas las actividades desarrolladas para United Capital por personal que pertenece a empresas proveedoras se encuadran en los contratos de provisión de servicios que vinculan a United Capital con estos proveedores.

1.1.3 La empresa proveedora proporcionará a United Capital en caso de cambios de personal los perfiles, funciones y responsabilidades asociados al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

1.1.4 Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo con lo establecido en el correspondiente contrato de servicios, así como a las normas y procedimientos establecidos a tal efecto entre United Capital y el proveedor.

1.1.5 El proveedor deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio propuesto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las presentes Políticas de Seguridad.

1.1.6 Se deberá realizar una evaluación de riesgos de seguridad asociados al servicio entregado por el proveedor, con la finalidad de identificar brechas que puedan ser potenciales vulnerabilidades que expongan la continuidad operativa de los procesos o puedan dañar la imagen Institucional,

para lo cual el área requirente en conjunto con el Encargado de Seguridad de la Información, deberán realizar este análisis previo a la contratación del servicio o adquisición del producto.

1.1.7 En caso de incumplimiento de cualquiera de estas obligaciones, United Capital se reserva el derecho de excluir a dicho personal de los accesos respectivos para las labores realizadas a favor de United Capital, debiendo el proveedor sustituir de inmediato al indicado personal; asimismo, United Capital se reserva el derecho de adoptar las medidas sancionadoras que se considere pertinentes contra el proveedor en cuestión y que se aplicarán en base a la cláusula de penalización establecida en el contrato de servicios suscrito, pudiendo UC llegar a la resolución de la relación contractual sin responsabilidad para esta última. Asimismo, United Capital se reserva la potestad de incluir los incidentes de seguridad en los certificados de ejecución de servicios que las empresas adjudicatarias pudieran solicitar.

1.1.8 Cualquier tipo de intercambio de información que se produzca entre United Capital y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

1.1.9 De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información.

1.1.10 Para los casos de desarrollo de sistemas de información para United Capital la Institución, se deberá considerar la revisión de los productos elaborados a partir de revisiones técnicas por parte del Departamento de Tecnología.

1.1.11 Para los casos que los sistemas de información sean expuestos a la red de Internet, se deberá considerar además la ejecución de pruebas de seguridad que permitan garantizar razonablemente la confidencialidad, integridad y disponibilidad de los datos manipulados en el sistema.

1.1.12 El acceso físico por parte de los proveedores a los activos de información deberá ser controlado y supervisado por personal del departamento de tecnología.

1.1.13 En las áreas protegidas o de alto riesgo, se deberán establecer procedimientos documentados formales que tengan por objeto gestionar la forma en que se realizarán los trabajos en su interior, el que deberá contar con medidas de registro de proveedores, como también controles detectivos, preventivos y correctivos.

1.1.14 Los proveedores podrán acceder en forma remota a los activos tecnológicos de United Capital a través de herramientas de conexión remota o Red Privada Virtual (VPN), cuando ello fuere necesario para el cumplimiento de las obligaciones que emanan del contrato de servicios.

1.1.15 En cualquier caso, todos los accesos serán gestionados por el Departamento de Tecnología y autorizado por Seguridad de la información y sólo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo.

1.1.16 Se deberá implementar controles que permitan limitar su acceso, registrar acciones para seguimiento y/o, supervisar visualmente el trabajo realizado.

1.1.17 Deberá existir un registro de los accesos que se han realizado a través de las herramientas señaladas en el párrafo primero de este apartado para efectos de trazabilidad y posterior revisión en caso de ser requerido.

2. CONFIDENCIALIDAD DE LA INFORMACION

2.1.1 El personal externo que tenga acceso a información de United Capital deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de United Capital a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por United Capital.

2.1.2 El personal externo que tenga acceso a información de United Capital evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.

2.1.3 El personal externo que tenga acceso a información de United Capital estará sujeto a los acuerdos de confidencialidad y no deberá compartir ningún tipo de información de carácter confidencial de UC, salvo que esté debidamente autorizado por esta.

2.1.4 El personal externo que tenga acceso a información de United Capital minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.

2.1.5 En relación con la utilización de agendas de contactos, de las herramientas ofimáticas dispuestas por United Capital, el personal únicamente introducirá datos personales como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, y teléfono.

2.1.6 Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, material o información propia o confiada de United Capital.

2.1.7 En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de propiedad o copia sobre dicha información. Asimismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación contractual entre el proveedor y United Capital. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de United Capital no supondrá, en ningún caso, una modificación de este punto.

2.1.8 Todas las obligaciones sobre los acuerdos de confidencialidad continuarán vigentes 5 años tras la finalización de las actividades en United Capital.

2.1.9 Cuando la VPN o cualquier otro tipo de conexión con una tercera parte represente un riesgo para la integridad y confidencialidad de la información de United Capital, se procederá a la desconexión y se notificara por las vías correspondientes las causas que originaron la misma, y en ningún caso

se podrá restablecer dicha conexión a menos que sea presentada la evidencia de que fue eliminada la causa que origino dicha desconexión.

2.1.10 El proveedor sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

2.1.11 Los dispositivos tecnológicos, tales como discos duros, pendrive u otros que contengan datos de carácter personal de clientes, relacionados o terceros, deberán almacenarse en un lugar de acceso restringido y solo otorgar acceso al personal autorizado.

3. INTERCAMBIO DE INFORMACION

3.1.1 Ninguna persona debe ocultar o manipular su identidad en ninguna circunstancia.

3.1.2 La distribución de información ya sea en formato digital o papel se realizará mediante los recursos determinados en el contrato de servicios. United Capital se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos recursos de difusión.

En relación con el intercambio de información dentro del marco del contrato de prestación de servicios, las siguientes actividades se considerarán como no autorizadas para el proveedor y sus empleados o personal de apoyo:

3.1.3 Transmisión o recepción de material protegido que infrinja la Ley de derecho de autor

3.1.4 Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

3.1.5 Transferencia de información a terceras partes no autorizadas de material de United Capital o material que es de alguna u otra manera confidencial.

3.1.6 Transmisión o recepción de información que infrinja la política de protección de Datos de United Capital.

3.1.7 Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.

3.1.8 Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el servicio contratado.

3.1.9 Todas las actividades que puedan dañar la buena reputación de United Capital están prohibidas en Internet y en cualquier otro lugar.

3.1.10 La transmisión de datos de carácter confidencial, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no pueda ser manipulada por terceros.

4. RESPONSABILIDADES DEL USUARIO

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolle labores para United Capital respete los siguientes principios básicos dentro de su actividad:

4.1.1 Cada persona con acceso a información de United Capital es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse ni compartirse con el resto del personal bajo ningún concepto.

4.1.2 Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.

Cualquier persona con acceso a información de United Capital deberá cumplir las siguientes directivas en relación con la gestión de las contraseñas:

4.1.3 solicitar el cambio de la contraseña siempre que exista un posible indicio de compromiso de los sistemas o de las credenciales de acceso.

4.1.4 Cambiar las contraseñas periódicamente y evitar reutilizar anteriores.

4.1.5 Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (“login”).

4.1.6 Notificar inmediatamente cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.

4.1.7 Cualquier persona con acceso a información de United Capital deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.

5. COMUNICACIÓN DE INCIDENCIAS

5.1.1 Todos los proveedores de servicios que cuenten con acceso (tanto privilegiado como no privilegiado) a los sistemas de información de United Capital que se realicen mediante el uso de infraestructura Tecnológicas de United Capital independientemente del lugar en el que se presten deberán cumplir con lo siguiente:

5.1.2 La persona que detecte cualquier incidencia deberá ponerse en contacto con el Departamento de Seguridad de la Información y Tecnología mediante correo electrónico TI_Seguridad@unitedcapitaldr.com u contacto telefónico 8098072000 extensiones 2058, 2017, 2053.

5.1.3 Se deberá notificar cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos o dispositivos que contengan información, sospechas de uso indebido del acceso autorizado por otras personas, suplantación de identidad u otros.

6. ARQUITECTURA DE SEGURIDAD

Todos los proveedores de servicios que cuenten con acceso (tanto privilegiado como no privilegiado) a los sistemas de información de United Capital y que se presten mediante el uso de infraestructura tecnológica del proveedor, deberán garantizar que se cumplen los siguientes requisitos de seguridad:

6.1.1 Siempre que el proveedor de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para United Capital o con datos propiedad de United Capital, los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese información propiedad de United Capital.

6.1.2 Todos los accesos a los sistemas de información que alberguen o procesen información propiedad de United Capital deberán estar protegidos, al menos, por un Firewall, que limite la capacidad de conexión a estos.

6.1.3 Los sistemas de información que alberguen o procesen información responsabilidad de United Capital especialmente sensible deberán estar aislados del resto.

6.1.4 Los sistemas de información utilizados para la prestación de servicios a United Capital deberán contar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

7. DISPONIBILIDAD DE SISTEMAS

Todos los proveedores de servicios que se presten mediante el uso de infraestructura tecnológica del proveedor deberán garantizar que se cumplen, al menos lo siguientes:

7.1.1 El proveedor del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información propiedad de United Capital se gestiona adecuadamente, evitando potenciales interrupciones o mal funcionamientos de dichos sistemas por saturación de recursos.

8. CONTROL Y GESTION DE IDENTIDADES

Todos los usuarios con acceso a los sistemas de información de United Capital dispondrán de una autorización de acceso unipersonal compuesta de identificador de usuario y contraseña. Esta obligación deberá ser cumplida tanto por todos usuarios, sean estos privilegiados o no. Adicionalmente, se contemplan los siguientes mecanismos de control:

8.1.1 Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

8.1.2 Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

8.1.3 Las credenciales de acceso no deben ser compartidas

8.1.4 Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

8.1.5 La longitud mínima de la contraseña deberá ser de 10 caracteres.

8.1.6 Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos

9. GESTION DE CAMBIOS

Todos los proveedores que presten servicio utilizando su infraestructura tecnológica y que impliquen el acceso (tanto privilegiado como no privilegiado) a los sistemas de información de United Capital deberán garantizar que se cumplen con la política de gestión de cambios de United Capital acatando lo siguiente:

9.1.1 Todos los cambios en la infraestructura tecnológica deberán estar controlados y autorizados.

9.1.2 Se debe completar el formulario de control de cambios para externos en el cual se especifica el tipo de cambio, el impacto que tiene, si existiese una indisponibilidad en los sistemas, la persona que valida del cambio, el personal que ejecuta el cambio, la fecha propuesta del cambio, el cronograma de actividades, persona que solicita el cambio y una descripción detallada del cambio.

9.1.3 Se deberán verificar o certificar que todos los cambios sobre las infraestructuras críticas, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos procesos o sobre su seguridad.

9.1.4 Se debe contemplar antes del cambio realizar respaldos, snapshot o replicación, que otorguen la capacidad de realizar rollback.

10. DESARROLLO DE SOFTWARE

Todos los proveedores de servicios que cuenten con acceso (tanto privilegiado como no privilegiado) a los sistemas de información de United Capital y que realicen actividades de desarrollo de aplicativos deberán garantizar que se cumplen, al menos, las siguientes condiciones:

10.1.1 Todo el proceso de desarrollo de software externalizado será controlado y supervisado por United Capital, y se desarrollará de acuerdo con la política interna de desarrollo de software, bajo una metodología de desarrollo seguro.

10.1.2 Se incorporarán mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida del diseño, desarrollo, implementación y operación de los aplicativos.

10.1.3 Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.

10.1.4 Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.

10.1.5 Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.

10.1.6 Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.

10.1.7 Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.

10.1.8 El acceso al código fuente de los aplicativos deberá estar limitado al personal que por sus funciones lo requiera.

10.1.9 Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.

10.1.10 En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.

10.1.11 Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

10.1.12 Sólo se transferirán al entorno de producción aquellos cambios en aplicativos que hayan sido probados, certificados y expresamente aprobados.

11. RESILIENCIA

Todos los proveedores de servicios que se presten mediante el uso de infraestructura tecnológica del proveedor deberán garantizar que se cumplen, al menos, con lo siguiente:

11.1.1 Los servicios cuentan con un plan de recuperación ante desastres probado que permite su continuidad ante algún caso de contingencia.

11.1.2 El plan de continuidad de negocios ha sido desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.

11.1.3 El proveedor puede demostrar la viabilidad del plan de contingencias.

12. REQUISITOS DE SEGURIDAD DE LA INFORMACION PARA PROVEEDORES

Los contratos con los proveedores para los casos que apliquen deberán abordar los temas sobre la mejora continua y las actualizaciones a los sistemas para evitar vulnerabilidades surgidas por la obsolescencia de uso de librerías desactualizadas u algún otro componente del sistema.

Adicional a los requerimientos de la Política de Proveedores y Debida Diligencia para su selección y contratación, United Capital solicitará la siguiente documentación al momento de establecer una relación de servicio con proveedores:

Requisitos para Desarrolladores:

12.1.1 Reporte de auditoría independiente (SOC2, SAE18) sobre la madurez de los controles implementados en la organización;

12.1.2 Evidencia de haber adoptado alguna metodología de desarrollo seguro;

12.1.3 Evidencia de ambiente de infraestructura de desarrollo separado del ambiente de producción

12.1.4 Tener definido e implementado un control de versiones;
12.1.5 Evidencia de poseer sistemas de control de cambio;
12.1.6 Evidencia del ambiente de QA y certificación de los cambios solicitados por United Capital;
12.1.7 Plan de continuidad de negocios y recuperación ante desastres;
12.1.8 Evidencia de haber adoptado algún estándar de mejores prácticas en materia de seguridad de la información, tecnología y riesgos como por ejemplo ISO, NIST, COSO, ITIL;
12.1.9 Tener implementado algún sistema de gestión de tickets;
12.1.10 Contrato Acuerdos de niveles de Servicios;
12.1.11 Firmar Acuerdo de confidencialidad de United Capital;
12.1.12 Completar el formulario de Requisitos de Seguridad de la información para proveedores

Requisitos para Implementadores de soluciones:

12.1.13 Un reporte de auditoría independiente (SOC2, SAE18) sobre la madurez de los controles implementados en la organización;
12.1.14 Evidencia de cumplimiento de algún estándar de mejores prácticas en materia de seguridad de la información, tecnología y riesgos como por ejemplo (ISO, NIST, COSO, ITIL, COBIT);
12.1.15 Tener implementado algún sistema de gestión de tickets;
12.1.16 Contar con un Plan de continuidad de negocios y recuperación ante desastres;
12.1.17 Contrato de Acuerdos de Niveles de Servicios;
12.1.18 Firmar Acuerdo de confidencialidad;
12.1.19 Completar el formulario de Requisitos de Seguridad de la información para proveedores

13. MANTENIMIENTO Y CONTROL DE ACTUALIZACIÓN

Versión	Fecha	Preparado por	Razón de actualización
V.1.1	Agosto 2021	Junior Ortiz Lahoz	Documento inicial

14. APROBACIONES E HISTORIAL DE REVISIONES

	Puesto	Firma	Fecha
Preparado	Gerente Cumplimiento		Octubre 2021
Revisado	Oficial de Ciberseguridad		Octubre 2021
Revisado	Gerente de TI		Octubre 2021
Revisado	Gerente de Riesgo		Octubre 2021
Aprobado	Gerente General		Octubre 2021