|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Logo Empresa | **POLÍTICAS DE SEGURIDAD INFORMÁTICA** | **Código** | TI-SEG-01 | |
| **Fecha** | 10 de sept. de 2019 | |
| **Versión** | 1 | Pagina 1 de 13 |

Tabla de contenido

|  |  |  |
| --- | --- | --- |
| 1. | Política global de seguridad de la información | 2 |
| 2. | Sanciones para las violaciones a las políticas de seguridad de la información | 3 |
| 3. | Criterios de las políticas de control | 3 |
| 4. | Políticas | 4 |

1. **POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN.**

La empresa reconoce que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades mas significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La empresa reconoce que toda la organización se encuentra expuesta a amenazas o peligros de diversos orígenes. Incluye siniestros. Como seria el caso de un incendio fortuito o intencional, acciones contra la integridad económica de la organización, como seria el caso de fraude, o las mas comunes de las amenazas materializadas en un error u omisión cometido por las personas en el normal desenvolvimiento de sus tareas. Igualmente, estas amenazas pueden ser de tipo accidental, cuando no existe un deliberado intento de perjudicar a la organización; o de tipo intencional, cuando su móvil es perjudicar a la compañía u obtener beneficios a favor de quien comete la acción.

Consiente de las necesidades actuales, la empresa implementa un modelo de gestión de seguridad de la información como la herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información, estableciendo una cultura de seguridad y garantizar el cumplimiento de los requerimientos, legales, contractuales, regulatorios y de negocio vigentes.

Los controles relacionados a la seguridad se establecen para impedir el acceso físico y lógico a los sistemas de información y los recursos relacionados, por parte de personas que no cuentan con autorización, como también reduce el riesgo que las personas autorizadas cambien o destruyan los datos.

Estos controles se establecen mediante la implementación de un conjunto de medidas preventivas, disuasivas, detectivas, y correctivas, destinadas a proteger la integridad, disponibilidad, confidencialidad y privacidad de la información de esta compañía.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios, y recursos de procesamiento de la información de la empresa, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con este, con el fin de mantener la confidencialidad, la integridad y así asegurar la disponibilidad de la información.

Por lo anterior cualquier violación a las políticas que en este documento se presentan, dará lugar a la aplicación de las acciones establecidas en el reglamento interno de trabajo de la empresa sin perjuicio de la aplicación de las demás acciones legales a que haya lugar por las autoridades competentes.

El comité de seguridad tendrá la potestad de modificar la política global o las políticas especificas de seguridad de la información, de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de estas.

1. **SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

Las políticas de la seguridad de la información pretenden instruir y afianzar la cultura de la seguridad de la información entre los funcionarios, personas externas y proveedores de la empresa. Por tal razón es necesario que las violaciones a las políticas de seguridad de la información sean clasificadas, con el fin de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

1. **CRITERIOS DE LAS POLÍTICAS DE CONTROL**

Para lograr los objetivos organizacionales soportados en IT, la empresa se propone que los controles generales cumplan los siguientes criterios:

* Preservar los atributos de la información: integridad, privacidad, exactitud y disponibilidad.
* Asegurar que la información generada y almacenada mediante el empleo de la tecnología de la información, conserva los atributos necesarios para ser útil y confiable a la organización.
* Apoyar la protección del patrimonio.
* Apoyar las medidas de protección para los bienes e inversiones de la organización mediante el uso adecuado de la tecnología de la información.
* Proteger la infraestructura tecnológica.
* Proteger todos los recursos que conforman la infraestructura tecnológica de la organización para preservar su integridad y funcionalidad.
* Apoyar la eficiencia operativa.
* Emplear la tecnología de la información como soporte a la eficiencia de la operación de la organización.
* Emplear los recursos de TI adecuadamente.
* Utilizar la totalidad de los recursos de la Tecnología de la Información en una forma legal, eficiente, eficaz y económica, de acuerdo con las características y a los objetivos institucionales de la organización.
* Brindar apoyo competitivo.
* Proporcionar soporte tecnológico competitivo a la operación y a la toma de decisiones de la organización en forma alineada a las políticas establecidas por la administración de esta.
* Mantener una cultura informática adecuada.
* Contar con una cultura informática competitiva en la organización, y acorde a las expectativas derivadas de los objetivos institucionales.
* Mantener una cultura organizacional adecuada.
* Mantener una cultura organizacional en el personal de tecnología de la información adecuada y alineada a la cultura institucional.
* Habilitar mecanismos de equilibrio.
* Utilizar la tecnología de la información como habilitador de mecanismos efectivos para la adecuación al medio ambiente y mantener el equilibrio interno en la organización.
* Mantener la continuidad y consistencia.
* Mantener la continuidad y consistencia del soporte tecnológico a la operación de la organización, tanto en la operación cotidiana como a mediano y largo plazo.
* Preservar las condiciones de la información.
* Mantener las condiciones de confidencialidad, integridad y disponibilidad de la información de la organización que se procese, almacene o genere utilizando Tecnología de la Información.

Con el cumplimiento de estos criterios se podrá estar en condiciones de asegurar razonablemente el logro de los siguientes objetivos dentro de la organización:

1. Calidad de la información que brindan los sistemas.
2. Alineamiento con los objetivos de la organización.
3. Calidad técnica de los sistemas.
4. Disponibilidad, integridad y confidencialidad de los sistemas.
5. Calidad del servicio informático.
6. Soporte adecuado a los sistemas.
7. Minimización o eliminación de los riesgos.
8. **POLÍTICAS**

Las siguientes normas de uso y manejo de aplicaciones, servicios y herramientas son de cumplimiento requerido a todos los empleados y usuarios de los recursos de la empresa.

**Consideraciones Generales**

* Los equipos propiedad de la empresa proporcionados a sus funcionarios y/o contratistas, y la infraestructura que los soportan, son para la ejecución exclusiva de sus labores asignadas y su configuración de Hardware y Software están de acuerdo a las labores inherentes a su cargo. Por lo tanto, el uso de estos recursos para actividades diferentes al cumplimiento de sus funciones será considerado un uso inapropiado.
* Los equipos e infraestructura de la empresa no puede ser utilizada para almacenar, copiar o distribuir música y videos en cualquier formato (MP3, WAV, AVI, MKV o similares) u otro tipo de material con protección y Derechos de Autor. Dado que la empresa acata y respeta las leyes de Propiedad Intelectual y Derechos de Autor, la posesión y distribución de música y videos en dichos formatos podrá acarrearle al usuario sanciones de tipo disciplinario y legal.
* La red eléctrica regulada identificada con tomas de color naranja es para uso exclusivo de equipos de cómputo. Esta red no puede ser utilizada para conectar equipos tales como herramientas, electrodomésticos, impresoras láser, equipos de iluminación, etc. En caso de requerirse utilizar un equipo de estos elementos, se debe consultar previamente a la Dirección de Tecnología.
* Los usuarios de equipos deben asegurarse de apagar o bloquear el computador e impresoras en el momento de ausentarse de su puesto de trabajo para evitar accesos no autorizados a la red e información interna.
* Todos los requerimientos de Servicio deben ser solicitados a través del Sistema de Help Desk para permitir el seguimiento al servicio solicitado.
* Los cambios de configuración en software o hardware de equipos de cómputo deben ser conducidos a través de IT.
* Los usuarios de equipos de la empresa, deben aplicar las prácticas comunes para el cuidado y preservación de las máquinas a su cargo, buscando mantenerlas en el mejor estado posible. Estas prácticas incluyen: (i) No consumir o manipular alimentos líquidos o sólidos cerca de los equipos de cómputo para evitar daños accidentales del equipo de computo, (ii) los equipos no deben ser limpiados con elementos que puedan deteriorar su apariencia o funcionamiento, (iii) no mover o desconectar el equipo de cómputo o algunos de sus dispositivos cuando se encuentre encendido, (iv) no destruir elementos de identificación o licenciamiento de los equipos como las licencias o plaquetas de inventario adheridas al chasis del computador y todas las demás normas básicas de cuidado.

**Instalación de Hardware y Software**

* No se deben instalar programas o máquinas virtuales sin la autorización de la Dirección de Tecnología. El software debe estar siempre debidamente soportado por una licencia de uso. La Dirección de Tecnología podrá hacer inventarios remotos o presenciales sobre el software instalado en las máquinas de la empresa. Las irregularidades son consideradas falta grave y serán reportadas a la Dirección de Gestión Humana, y CFO de la empresa.
* En caso de requerirse un software determinado por razones del negocio, el correspondiente Director o Gerente de Empresa gestionará la aprobación de su uso con la Dirección de Tecnología que se encargará de evaluar la necesidad del software y su valor de adquisición. Una vez sea aprobada la solicitud por parte del Director o Gerente, por parte del CFO y si aplica, se procederá a adquirir e instalar el software. Los medios y códigos de licencia o activación del software serán custodiados por la Dirección de Tecnología.
* No es permitida la carga o descarga de software de internet o por cualquier otro medio que viole las leyes de Propiedad Intelectual y Derechos de Autor. La Dirección de Tecnología es la única autorizada para descargar software de Internet. Si alguien requiere de este servicio, debe solicitarlo por escrito a ésta Dirección con la justificación y confirmación de que es de libre uso antes de ser descargado e instalado.
* No está autorizado tener en los puestos de trabajo ningún tipo de software, aplicación o archivo, de carácter personal o corporativo, que este sujeto a condiciones legales para su uso y que no se ajuste completamente a las normas de esta política y las políticas globales de la empresa. Aplica para bienes e información en cualquier medio magnético (discos duros externos), ópticos (CDs, DVDs) o memorias USB.
* El empleado que aloje o haga uso de cualquier tipo de software u otro elemento sin cumplir los requisitos de su licencia de uso, estará expuesto a las acciones establecidas en el Reglamento Interno de Trabajo *-* aprobado por el Ministerio de Protección Social que incluye sanciones que pueden ir hasta la cancelación por causa justa de su contrato.
* Cada funcionario o usuario registra los recursos de cómputo que le son asignados en el Formato de Inventario del Software y Hardware. En este documento se relaciona la plaqueta de inventario única de cada computador y el software licenciado que se deja instalado.
* Las licencias de software que se encuentre en medios físicos deben ser almacenadas en un lugar seguro y La Dirección de Tecnología conservará copias para control o requerimientos externos.
* El software adquirido y desarrollado por funcionarios de la empresa es exclusivo para el funcionamiento de las operaciones de la compañía, y en ningún momento debe ser copiado o prestado para otros fines distintos a los que se adquirieron o se desarrollaron. En caso de que terceros requieran de éstos, debe ser autorizado por el CFO.
* Los traslados de equipos de cómputo entre dependencias, empresas o los cambios de responsable asignado, deben hacerse en coordinación de la Dirección de Tecnología. No es permitido que los empleados intercambien equipos y/o sus periféricos (teclados o ratones) o cambien equipos de ubicación.
* La empresa no es dueño del software licenciado, ni de la documentación adjunta con el software, a menos que así lo autorice el titular de la propiedad intelectual y los Derechos de Autor. Ningún empleado tiene el derecho de reproducirlos a menos que sea la copia de respaldo. Las licencias que posee la empresa, solo le otorgan el derecho al uso del software dentro de la compañía.
* Los empleados deberán usar el software solamente de la manera establecida en la licencia por el fabricante.
* Es responsabilidad de cada empleado notificar a la Dirección de Tecnología de cualquier uso indebido de software o de su documentación relacionada dentro de la empresa.
* Para proteger la propiedad intelectual de la compañía, no está permitido extraer o divulgar a personal no autorizado información que tenga relación con nuestra operación, sin permiso expreso y por escrito.
* No Está permitido compartir lógicamente discos o carpetas de los computadores a usuarios. Ni está permitido compartir los recursos de los computadores cuando se entreguen permisos a todos los usuarios.
* Cualquier acceso o intento de acceso para cambiar las claves de administrador local o de administrador de dominio mediante el uso de herramientas de hacking o fuerza bruta, será considerado falta grave y será reportado a la Dirección de Gestión Humana, y al CFO.

**Manejo de Correo Electrónico e Internet**

* El correo interno y la Internet deben ser utilizados exclusivamente en las operaciones de la compañía.
* El correo no se debe utilizar para enviar mensajes en cadena o mensajes con contenido sensible de intolerancia, violencia, discriminación, ofensivo, malintencionado, pornográfico o en contra de las buenas costumbres. En general, el correo es de uso empresarial y no personal.
* Como tal el servicio de correo Outlook en el paquete Office 365 solo permite el envío de correos de máximo 15 Mbytes. En el evento que un funcionario requiera enviar archivos de más de 15 Mbytes, deberá hacerlo a través de medios externos como CDs, DVDs, etc. o copiarlo en la carpeta pública del área del funcionario para quien va dirigido, o comprimirlos antes de ser enviados. En caso de envío de información a clientes se debe solicitar a la Dirección de Tecnología la habilitación de un servicio FTP o similar (BOX) para una carga o descarga más controlada.
* Cada usuario es responsable de almacenar en el disco duro los documentos importantes del correo, teniendo en cuenta que el correo es un sitio de intercambio de información más no un sitio de almacenamiento de información (teniendo un almacenamiento de 3 meses únicamente). Una vez almacenado en el disco debe ser eliminado del correo.
* No está permitido usar la red corporativa para consultar, divulgar o promover lugares en Internet u otra red a la que la empresa tenga acceso con contenido de intolerancia, violencia, discriminación, ofensiva, malintencionada, pornográfica o en contra de las buenas costumbres.
* El uso de la red de internet debe ser usada exclusivamente con fines laborales.

**Copias de Seguridad de La información**

Con el fin de proteger la información procesada en los aplicativos en la empresa se establecen las siguientes normas con respecto a copias de seguridad de los sistemas de información.

* La Dirección de Tecnología mantendrá una copia de seguridad actualizada semanalmente de la información de los aplicativos claves de la compañía en un lugar externo a las instalaciones de la empresa la cual permita recuperar la información en caso de una contingencia (Plan DRP).
* Es responsabilidad del área de IT, realizar una copia de seguridad de los archivos de trabajo residentes en los computadores actualizada máximo cada semana. Para tal efecto se tiene destinada una ruta por usuario con time machine o backup de Windows automática. Se prohíbe la copia de documentos personales, fotografías personales, imágenes pornográficas, música, juegos o cualquier tipo de archivo no relacionado con las labores relacionadas con su cargo y que pueda poner en riesgo a la compañía al violar las leyes de Derechos de Autor.
* Todos los funcionarios que laboren fuera de las oficinas de la empresa por tiempos prolongados deben asegurarse de que toda la información valiosa que necesiten salvar quede almacenada en el servidor de archivos o en la nube corporativa aprobada por la Dirección de Tecnología.

**Control de Claves de Acceso**

* Cada funcionario debe tener su Clave de Acceso que le permitirá ingresar de forma exclusiva a los aplicativos que está autorizado, siendo esta clave personal e intransferible. Esta clave es exclusiva de cada funcionario y es su responsabilidad mantenerla en secreto, ya que cualquier modificación, daño o acceso que ocurra y se detecte que fue por indebido manejo de su clave, lo hace responsable de las acciones de tipo legal y disciplinario que esto conlleve. Cada cuenta debe seguir los siguientes lineamientos:

1. La contraseña de la cuenta debe ser cambiada, mínimo cada 30 días y máximo cada 90 días, y en ningún momento debe ser igual a la anterior.
2. La longitud de la contraseña debe ser como mínimo de ocho caracteres.
3. La contraseña debe ser compleja. Debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial y debe ser diferente al nombre del usuario.
4. Se mantendrá un histórico de hasta tres cuentas en el controlador de dominio. Es decir, que el funcionario no podrá utilizar ninguna de las tres contraseñas anteriores.
5. Se enviará una notificación de cambio de contraseña: 7 días antes de que la contraseña se bloquee, para que el funcionario la cambie.

* En cuanto al manejo de las claves para ingresar al sistema de información AdvertMind, el usuario debe cambiar su clave de acceso cada vez que lo estime conveniente o máximo cuando se cumpla el plazo fijado en el numeral anterior.
* Para controlar el ingreso a los servicios de red del dominio, las claves de acceso al sistema serán deshabilitadas después de tres intentos fallidos. En este caso el funcionario debe informarle al Personal de la Dirección de Tecnología, para realizar su respectivo desbloqueo.
* La Dirección de Gestión Humana es el área responsable de solicitar a la Dirección de Tecnología el acceso a la red, el correo, el sistema AdvertMind u otro sistema que requiera una cuenta de acceso una vez se tenga confirmación de la contratación de personal nuevo o de reemplazo. Esta solicitud debe realizarse a través de sistema HELP DESK con mínimo 5 días de antelación. Así mismo en caso de un retiro del funcionario debe ser solicitado por el mismo sistema de HELP DESK a la Dirección de Tecnología, esta solicitud debe darse con un mínimo de 5 días para garantizar que el retiro de cuentas sea realizado antes de 24 horas. En caso de que el usuario requiera algún permiso en especial o algún cambio en la configuración del perfil debe ser solicitado por el jefe directo, gerente o director del área encargado al área de Tecnología.
* Cada vez que un funcionario se retire de su puesto de trabajo debe bloquear su sesión con el fin de evitar que usuarios malintencionados realicen acciones indeseadas con dicha cuenta.
* **Consideración especial:** Para el caso de los identificadores genéricos o por defecto en cada aplicación, el administrador de seguridad de esta deberá eliminarlos de ser posible. En caso contrario, el Director de Tecnología o administrador del sistema debe firmar un documento en el cual se hace responsable por el manejo confidencial de dichas claves de acceso. Deberá cambiar la contraseña por uno diferente al asignado por defecto (de ser la primera vez). Este cambio de contraseña se deberá realizar periódicamente.
* Todos los accesos de los funcionarios a sus equipos de cómputo tienen privilegios de usuario estándar. Sólo la Dirección de Tecnología tiene privilegios de administrador en todos los equipos. En caso de que, motivado en un requerimiento de sus funciones, un usuario necesite privilegios administrativos sobre su máquina, deberá hacer su solicitud justificada a través de la Gerencia o Dirección de su área y/o empresa a la Dirección de Tecnología. En caso de otorgarse privilegios administrativos, el funcionario a cargo de la máquina se hace responsable de velar por el cumplimiento de esta política sobre el equipo. Para tal efecto firmará un formato asumiendo esta responsabilidad.

**Control de Virus Informáticos**

* La compañía mantendrá instalado en sus equipos de cómputo un software antivirus que garantice la seguridad en la información, el cual se actualizará diariamente a través de la red.
* La Dirección de Tecnología es responsable de actualizar el antivirus de la red semanalmente o antes, si es necesario.
* En caso de que se detecte la presencia de un virus en algún archivo recibido por cualquier fuente (correo interno, USB, Internet etc.), éste debe eliminarse y se debe notificar el hecho a la Dirección de Tecnología, para que se tomen las acciones pertinentes.
* No es permitido interrumpir el proceso automático de actualización del Antivirus.
* Es responsabilidad de cada usuario no abrir o reenviar archivos de dudosa procedencia para evitar el contagio de virus. En caso de que se detecte un virus en un archivo recibido, este sin excepción debe ser eliminado y se debe informar a la Dirección de Tecnología para evaluar su impacto en los demás equipos o en la red.
* Con el fin de generar una mayor protección a la información corporativa, el sistema de antivirus podrá escanear diariamente los computadores de la red en busca de virus informáticos. Este escaneo se hará en modo sigiloso para que no afecte el trabajo de los usuarios. El reporte de este escaneo es enviado a la consola de administración del software antivirus.

**NOTA: No es permitido instalar antivirus diferentes a los proporcionados por la Empresa.**

**Requerimientos y/o Corrección de programas**

* En caso de que se presenten errores en los aplicativos de la empresa, estos deberán ser notificado a la Dirección de Tecnología a través del sistema de HELP DESK para tramitar la solución requerida. En este tiquete se deberán almacenar los registros de sistema documentados, las falencias encontradas y las acciones a desarrollar o desarrolladas con su respectiva fecha de ejecución.
* Si se requiere un nuevo desarrollo o una nueva funcionalidad para la empresa, se debe hacer un requerimiento a través de HELP DESK a la Dirección de Tecnología para su análisis de viabilidad y factibilidad. Si es del caso, y una vez sea aprobado, la Dirección de Tecnología procede a gestionar el desarrollo con el respectivo proveedor o a solicitar la implementación de la solución.

**Niveles de Seguridad**

Para evitar el acceso no autorizado a datos sensibles, se definieron y configuraron tres niveles básicos de seguridad que los usuarios deben pasar antes de acceder a dicha información, así:

* Seguridad de Acceso a la Red
* Seguridad de Acceso a los Sistemas de Información
* Seguridad de Acceso a las opciones de los menús de las aplicaciones que dependen de cada administrador de seguridad de cada aplicativo.

La dos primeras clasificaciones dependen de un login y password asignados por el administrador de red / administrador de seguridad de la aplicación respectivamente.

**Nota: Ningún funcionario de la Dirección de Tecnología puede usar contraseñas para el ingreso a los sistemas de información en producción, y tampoco puede solicitar a los usuarios finales le proporcionen sus contraseñas de acceso, en el caso de soporte técnico estás siempre deben ser ingresadas por el usuario responsable de la contraseña.**

**Control de Acceso a las Oficinas**

* Se restringe el acceso de contratistas, proveedores de materiales, vendedores y personas ajenas a la Dirección de Tecnología, al Centro de Cómputo donde están ubicados los Servidores, Planta Telefónica y Equipos de Comunicaciones.
* El Centro de Cómputo permanecerá cerrado con llave o demás mecanismos de control de acceso como biométricos, lectores de tarjetas, etc, y estará ubicado en un lugar aislado de los puestos de trabajo de los funcionarios de la compañía.
* Se restringe el ingreso de equipos de cómputo de propiedad de los funcionarios a las oficinas de la empresa, para inspección o reparación.

Si se requiere que personal externo de la compañía acceda a los centros de cómputo y cableado o a los sistemas de información, se debe generar una solicitud la Dirección de Tecnología, la cual contiene el Voto del Director Tecnología, en donde se detalle:

* Fecha de solicitud
* Nombre del proveedor.
* Nombre de consultor (es)
* No. Cédula
* Descripción de la labor que se desarrollará
* Tiempo (Fecha de Inicio / Fecha de finalización)
* Aplicaciones y recursos de tecnología para el desarrollo de sus labores (Indicando Niveles: Consulta, Actualización, Eliminación)
* Horarios
* Firma del acuerdo de confidencialidad
* Nombre y cargo de la persona de la empresa que realizará seguimiento y reportará las novedades del personal externo (Ej.: Notificación para que el usuario se elimine de la red corporativa, cambios de consultor, etc.)
* En cada centro de cómputo y cableado debe reposar una bitácora en donde se registren los visitantes, con fecha, hora de ingreso y actividad realizada.

**Ingreso de Computadores Personales**

El ingreso de computadores personales, de contratistas o proveedores a las instalaciones debe ser registrado. Para tal efecto se debe firmar el documento de responsabilidad personal sobre el software que se encuentre instalado en el computador que está siendo ingresado, librando a la empresa de responsabilidad alguna sobre el computador o los programas que contenga.

* Para conectar computadores personales, de proveedores o contratistas a la red corporativa, se debe solicitar autorización por parte del funcionario responsable a la Dirección de Tecnología por medio de Help Desk. Cualquier intento de acceso no autorizado a la red corporativa será considerado falta grave y el funcionario responsable del equipo personal, del proveedor o del contratista será reportado a la Dirección de Gestión Humana y al CFO.
* Cualquier intento de copia de información de la compañía a equipos personales, de contratistas o de proveedores, será considerado falta grave y será reportado a la Dirección de Gestión Humana y al CFO.