POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
ORALX CUCUTA LIMITADA

TABLA DE CONTENIDO

OBJETIVO

La presente Política de Seguridad de la Información (en adelante “Política de Seguridad”) tiene como objetivo establecer las políticas específicas de la seguridad de la información de **ORALX CUCUTA LTDA** (en adelante “ORAL X " o “la Empresa”), con el fin de regular la Gestión de la Seguridad y Confidencialidad de la Información al interior de la Empresa, protegiendo, preservando y administrando la Integridad, Confidencialidad y Disponibilidad de la Información para cumplir con lo dispuesto en las normativas referentes a la Protección de Datos Personales y las medidas de Seguridad de la Información.
Para tales propósitos, la presente Política de Seguridad contiene las medidas técnicas, humanas y administrativas necesarias para otorgar Seguridad a la Información e Información Personal mitigando de manera diligente el riesgo de su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

DESTINATARIOS

Las políticas específicas definidas en la presente Política de Seguridad deben ser aplicadas a todos los procesos estratégicos, misionales, de apoyo y de evaluación de ORAL X, y, por ende, deben ser puestas en conocimiento de todos los accionistas, directivos, empleados, contratistas y/o terceros que tengan una vinculación laboral y/o convenios o acuerdos de alguna clase con la misma. Asimismo, la presente Política de Seguridad debe ser tenida en cuenta en el diseño de nuevos procesos al interior de la Empresa.
La presente Política de Seguridad será parte integral tanto de los acuerdos laborales que firman los empleados de la Empresa, como de todos aquellos acuerdos y/o convenios con contratistas y/o terceros con los que se busque llevar a cabo una actividad puntual.

GLOSARIO

AMENAZA: posibilidad de ocurrencia de cualquier tipo de Evento o acción que puede producir un Incidente de Seguridad.
AUTORIZACIÓN: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales. La prueba de la Autorización deberá estar disponible para consultas posteriores de manera individualizada para cada Titular.
BASE DE DATOS: conjunto organizado de Datos Personales que sean objeto de Tratamiento.
CENTROS DE DATOS: ubicación física que almacena máquinas de computación y sus equipos de Hardware relacionados, así como las Bases de Datos físicas.
CIFRAR: método que permite aumentar la Seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
CÓDIGO MALICIOSO: programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de Información.
CONFIDENCIALIDAD: procesos para velar por la reserva de la Información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar el suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas.

CONTROL DE ACCESO BASADO EN ROLES: control que restringe el acceso a la red según el rol de un empleado dentro de la Empresa y se ha convertido en uno de los métodos principales para el control de acceso avanzado. Los roles en el Control de Acceso Basado en Roles están definidos por los niveles de acceso que los empleados tienen a la red.

DISPONIBILIDAD: medida de la frecuencia con que los datos y las aplicaciones están listos para poder acceder a ellos cuando se necesitan.

ENCARGADO DEL TRATAMIENTO: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del responsable del Tratamiento.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la Política de Seguridad o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. Toda violación a una Política de Seguridad de la Información de la entidad.

FINALIDAD: propósito para el cual es recolectada y será tratada la Información Personal.

HARDWARE: parte tangible de un sistema informático, que puede corresponder a componentes de tipo: mecánico, electrónico, eléctrico, o electromecánico.

INCIDENTE DE SEGURIDAD: fallas de seguridad respecto del Tratamiento de Datos Personales que pueden afectar su Confidencialidad, Integridad y Disponibilidad. En general, se entiende como Incidente de Seguridad cualquier forma de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los Datos Personales. Un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

INFORMACIÓN: toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro independientemente de si se trata de Información Personal, Información Personal Sensible, Información Confidencial, entre otros.

INFORMACIÓN O DATO PERSONALES: cualquier Información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional.

INFORMACIÓN PERSONAL SENSIBLE O DATOS PERSONALES SENSIBLES: Información Personal que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

INTEGRIDAD: característica técnica de Seguridad de la Información con la cual se salvaguarda la exactitud y totalidad de la Información y los métodos de procesamiento asociados a la misma. Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones.

INTRANET: red informática privada, que utiliza tecnologías de Internet (como TCP/IP, HTTP, etc.), implementada dentro de una organización para facilitar la comunicación interna, el acceso a la información y la colaboración entre sus miembros.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: responsable de planear, coordinar y administrar los procesos de Seguridad de la Información en la Empresa y de velar por el cumplimiento de las normas en materia de Protección de Datos Personales.

OFICIAL DE SISTEMAS: responsable de asegurar el correcto funcionamiento de los sistemas informáticos, tanto hardware como software, de la organización. Esto incluye servidores, redes, dispositivos móviles, aplicaciones, bases de datos y todo lo relacionado con el almacenamiento y procesamiento de la información.

OFICINA DE TECNOLOGÍA E INFORMÁTICA ("OTI"): grupo de trabajo compuesto por el Oficial de Seguridad de la Información y el Oficial de Sistemas, cuyo rol es diseñar organizar, coordinar, controlar y ejecutar procesos, procedimientos, planes, programas y proyectos para la implementación de los sistemas, normas y procedimientos de la informática requeridos por la entidad del desarrollo informático.

REGISTRO NACIONAL DE BASE DE DATOS ("RNBD"): directorio público de las Bases de Datos Personales sujetas a Tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos.

RESPONSABLE DEL TRATAMIENTO: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre las Bases de Datos y/o el Tratamiento de los Datos Personales. En el marco de la presente Política de Seguridad, se entiende que el responsable del Tratamiento es ORAL X

SEGURIDAD DE LA INFORMACIÓN: medidas técnicas, humanas y administrativas necesarias para la preservación de la Confidencialidad, la Integridad y la Disponibilidad de la Información y la Información Personal, al igual que todas las medidas de autenticidad, trazabilidad, *accountability*, no repudio y fiabilidad con el fin de disminuir los riesgos de su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO ("SIC"): autoridad de protección de datos en Colombia, a través de su Delegatura de Protección de Datos Personales.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo. Éste garantiza que las empresas tomen medidas sistemáticamente para mantener segura la Información, la Información Personal y la Información Personal Sensible.

SISTEMA DE INFORMACIÓN: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de Información según determinados procedimientos, tanto automatizados como manuales.

SISTEMA KUBAPP: aplicación utilizada por ORAL X para manejar, configurar, administrar y almacenar de manera centralizada y automatizada su Información e Información Personal. Integra el control de inventario, facturación, compras, cartera, cuentas por pagar, caja y contabilidad, entre otros.

TECNOLOGÍA DE LA INFORMACIÓN: Hardware y/o softwares operados por la Empresa, o por un tercero Encargado del Tratamiento que procese información en su nombre, para llevar a cabo una función propia de la Empresa independientemente de la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones o cualquier otro tipo.

TITULAR: persona natural cuya Información Personal sea objeto de Tratamiento.

TRATAMIENTO: cualquier operación o conjunto de operaciones sobre Información Personal, tales como la recolección, almacenamiento, uso, circulación o supresión.

TRANSFERENCIA: tiene lugar cuando el responsable del Tratamiento de Datos Personales, ubicado en Colombia, envía la Información Personal o los Datos Personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

TRANSMISIÓN: Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

USUARIO: todo directivo, empleado, contratista y/o tercero que tiene acceso a Información e Información Personal de la Entidad a través del Sistema Kubapp.

VULNERABILIDAD: capacidad o condiciones y características del Sistema Kubapp y/o de la Intranet que lo hace susceptible a Amenazas, con la posibilidad de que como resultado se pueda sufrir algún Evento o Incidente de Seguridad de la Información.

VIRTUAL PRIVATE NETWORK (“VPN”): tecnología de red que permite una extensión segura de la red local, sobre una red pública o no controlada como Internet.

WIFI: tecnología de comunicación inalámbrica que permite conectar a Internet equipos electrónicos, como computadoras, *tablets*, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la Información.

GENERALIDADES

La Información de ORAL X es un activo que se considera esencial para las actividades de la Empresa y debe ser protegido de acuerdo con los principios de Confidencialidad, Integridad y Disponibilidad, así como los demás principios incluidos en la Constitución y la Ley colombiana respecto a la intimidad de las personas y a la Protección de los Datos Personales.

En la medida en que ORAL X está comprometida con la implementación de altos estándares en materia de Seguridad de la Información y el cumplimiento de los principios antes mencionados, ha implementado un Sistema de Gestión de Seguridad de la Información que es transversal a todos los procesos y la estructura de la Empresa al igual que el diseño de sus procesos futuros, Sistemas de Información y controles internos. La presente Política de Seguridad es parte esencial del Sistema de Gestión de Seguridad que comprende, adicional a esta Política, otras medidas complementarias y por lo tanto debe leerse en conjunto con la Política de Tratamiento de Datos Personales y el Manual de Políticas y Procedimientos de ORAL X
La implementación del Sistema de Gestión de Seguridad está a cargo del Oficial de Seguridad de la Información de la Empresa.

POLÍTICAS ESPECÍFICAS

Política de Organización Interna

Objetivo: dar lineamientos sobre la estructura y organización interna de la Empresa para la implementación y operación de los procedimientos en materia de Seguridad de la Información dentro de ORAL X. Asimismo, esta política tiene como propósito definir de manera clara los roles y obligaciones de quienes tienen a cargo la Seguridad de la Información al interior de la Empresa.

Asamblea de Accionistas, Junta Directiva y otros Administradores

La Asamblea de Accionistas, la Junta Directiva y en general los administradores de ORAL X están comprometidos con el cumplimiento de todas las normas en materia de Seguridad de la Información y Protección de Datos Personales. Por lo tanto, de conformidad con la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Circular Externa No. 003 del 22 de agosto de 2024 de la SIC, se obligan a lo siguiente:

1. Revisar y aprobar la presente Política de Seguridad de la Información en el marco del Sistema de Gestión de Seguridad de la Información de la Empresa.
2. Aprobar las propuestas de implementación de medidas de Seguridad de la Información que sean necesarias para cumplir con la normatividad vigente en materia de Seguridad de la Información y Protección de Datos Personales.
3. Adoptar mecanismos internos para hacer cumplir las políticas internas establecidas.

4. Establecer los lineamientos corporativos adecuados para adoptar medidas precautorias o preventivas para proteger los derechos de los Titulares de los Datos Personales.
5. Establecer lineamientos para fortalecer continuamente las medidas de Seguridad de la Información.

Asistente Administrativa

La Asistente Administrativa es la oficina responsable de la gestión y administración de los procesos de contratación y pago de proveedores. Asimismo, la Asistente Administrativa es la encargada de supervisar la Coordinación de Talento Humano. Dentro de la Empresa, la Asistente Administrativa tendrá los siguientes roles, no obstante los demás que se puedan encontrar en el presente documento o en otros complementarios:

1. Gestionar la relación con los proveedores lo que incluye contratación, revisión de procesos de facturación y pago, entre otros.
2. Supervisar a las labores a cargo de Talento Humano.
3. Gestionar las referencias de candidatos a cargos al interior de la Empresa.
4. Verificar los antecedentes de todos los candidatos a un empleo en la Empresa de acuerdo con las leyes, reglamentos y ética pertinentes.
5. Supervisar que el proceso de contratación de empleados cumpla con las políticas y procedimientos en materia de Seguridad de la Información.
6. Realizar los procesos disciplinarios de los empleados cuando sea necesario.
7. Supervisar que la terminación de los contratos laborales se haga de manera adecuada.

Gerencia

La Gerencia es la oficina responsable de la gestión y administración de los recursos financieros, materiales y humanos de una empresa, para lograr los objetivos establecidos. Dentro de la Empresa, la Gerencia tendrá los siguientes roles, no obstante los demás que se puedan encontrar en el presente documento o en otros complementarios:

1. Autorizar el retiro de activos de Información físicos o digitales de las instalaciones de la Empresa.
2. Autorizar el ingreso de empleados, contratistas y terceros los fines de semana a las instalaciones de la Empresa.
3. Suscribir y ejecutar contratos con contratistas.
4. Autorizar el acceso a la Información a proveedores, contratistas y terceros cuando sea estrictamente necesario para que puedan cumplir con el objeto del contrato suscrito.
5. Autorizar el uso de ciertas páginas de Internet.
6. Permitir el acceso al lugar de custodia donde se almacena la Información de forma física.
7. Autorizar la toma de fotografías dentro de las instalaciones de la Empresa.
8. Solicitar de manera anual rendición de cuentas a Oficial de Seguridad de la Información y al Oficial de Sistemas sobre la implementación de los procesos indicados en la presente Política para incluirlo dentro de los respectivos informes

de gestión ante los directivos de la Empresa.

Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información es responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones para mejorar y fortalecer la Seguridad de la Información de la Empresa, basándose siempre en los principios de Confidencialidad, Integridad y Disponibilidad. Esto incluye, entre otros, identificar riesgos, diseñar e implementar medidas de Seguridad de la Información y de mitigación de riesgos, vigilar el adecuado cumplimiento normativo en cada proceso del negocio, monitorear sistemas, gestionar incidentes y capacitar al personal.

Dentro de la Empresa, el Oficial de Seguridad de la Información tendrá los siguientes roles, no obstante los demás que se puedan encontrar en el presente documento o en otros complementarios:

1. Mapear los canales por los cuales se está obteniendo la Información de la Empresa.
2. Clasificar los tipos de Información con los que cuenta la Empresa.
3. Establecer los lineamientos para proteger la Información y la Información Personal en todos los procesos de la Empresa.
4. Tener claridad sobre las plataformas, aplicaciones, repositorios o lugares físicos donde la Información se encuentra almacenada y sobre las medidas de Seguridad de la Información que le aplican.
5. Clasificar, cuando se trate de Información Personal, las Bases de Datos con las que cuenta la Empresa, determinar si son digitales o físicas, las medidas de Confidencialidad y Seguridad que le son aplicables y si se están cumpliendo para su obtención y Tratamiento todas las normas en materia de Protección de Datos Personales.
6. Determinar para todos los casos las personas autorizadas para acceder a la Información de la Empresa.
7. Controlar el acceso a la Información y los niveles de privilegio de los Usuarios.
8. Registrar y actualizar de forma correcta y oportuna el RNBD ante la SIC siguiendo lo establecido en el Manual de Políticas y Procedimientos de ORAL X y lo dispuesto en las normas aplicables.
9. Mantener contacto con las autoridades en materia de Protección de Datos y Seguridad de la Información cuando ello sea necesario.
10. Mantenerse actualizado respecto de las medidas de Seguridad de la Información adecuadas y aplicables al modelo de negocio de la Empresa.
11. Verificar el cumplimiento de las Política de Seguridad de la Información.
12. Llevar a cabo capacitaciones en Seguridad de la Información y Protección de Datos Personales.
13. Recibir y evaluar reportes de auditorías y evaluaciones de Seguridad de la Información.
14. Gestionar Incidentes de Seguridad de la Información conforme a lo dispuesto en el Manual de Políticas y Procedimientos.
15. Reportar Incidentes de Seguridad a la SIC a través del RNBD.
16. Documentar los requerimientos legales y contractuales relacionados con la Seguridad de la Información.
17. Realizar de manera periódica seguimiento a la corrección de Vulnerabilidades.
18. Aplicar el procedimiento de borrado seguro cuando ello sea necesario. En los casos de tratarse de Información Personal, el borrado sólo se hará cuando se cuente con la

autorización del Titular para ello o cuando se haya cumplido la Finalidad para el Tratamiento.

19. Realizar, en conjunto con el Oficial de Sistemas, el procedimiento de borrado seguro a los equipos informáticos devueltos por parte de empleados que terminen su relación laboral con la Empresa, con el fin de que la Información contenida no pueda ser recuperada posteriormente por quienes se desvinculan.
20. Elaboración de los Contratos de Trasferencia o de Transmisión con terceros cuando haya flujo de Información Personal cumpliendo con lo dispuesto por la ley 1581 de 2012 y el decreto 1377 de 2013 a este respecto.
21. Realizar una evaluación de riesgos que considere los riesgos del contrato con un proveedor, contratista o tercero en materia de Seguridad de la Información.
22. Integrar la Seguridad de la Información y la protección de los Datos Personales en la gestión de los proyectos en cualquier etapa en la que se encuentre de la Empresa, independientemente de su naturaleza, para asegurar que los riesgos de Seguridad de la Información sean mitigados de manera adecuada.
23. Desarrollar, en conjunto con el Oficial de Sistemas, el plan interno de *backups* en el que se establezca el tipo de Información a que se le debe aplicar el *backup*, cuándo se aplica, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de Información.
24. Dar las directrices sobre retención, almacenamiento, manipulación y eliminación y en general Tratamiento de Información e Información Personal.
25. Cumplir con los lineamientos para la protección contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de la Información, de acuerdo con los requisitos legales, reglamentarios y contractuales.
26. Llevar a cabo directamente, o a través de expertos externos, las capacitaciones correspondientes en materia de Seguridad de la Información y Protección de Datos Personales.
27. Planificar, definir el alcance y realizar auditorías periódicas a los sistemas de Información, asegurando que las pruebas no afecten la disponibilidad del sistema.
28. Monitorear y proteger los logs de auditoría y registros de control, garantizando su Integridad y Confidencialidad.
29. Documentar y presentar los resultados de las auditorías, protegiéndolos de accesos no autorizados.
30. Velar por el cumplimiento de las obligaciones en materia de Protección de Datos Personales y de Seguridad de la Información.
31. Tener en cuenta, como buena práctica, las recomendaciones de la Guía Oficial de Protección de Datos Personales (2023) https://www.sic.gov.co/sites/default/files/files/2023/Guia%20de%20datos%202023%20(2).pdf y aquellas incluidas en la Guía de Seguridad de la Información (2020) https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf entre otras relevantes para el buen desempeño de su labor.

Oficial de Sistemas

El Oficial de Sistemas es el responsable de la gestión, mantenimiento y seguridad de la infraestructura tecnológica e informática en ORAL X, lo que incluye, entre otros, el monitoreo del buen funcionamiento del Sistema Kubapp, de la Intranet y demás dispositivos de la Empresa. Dentro de la Empresa tendrá los siguientes roles, no obstante los demás que se puedan encontrar en el presente documento o en otros

complementarios:

1. Colaborar con el Oficial de Seguridad de la Información en la implementación de medidas de Seguridad de la Información.
2. Administrar desde el punto de vista técnico la gestión de claves de cifrado de los Usuarios en el Sistema Kubapp, lo que incluye la generación, distribución, revocación y protección de las claves, las cuales serán asignadas por la Gerencia.
3. Revisar de manera periódica la actualización de equipos.
4. Implementar mecanismos para la protección y prevención contra el software malicioso o cualquier otro tipo de acceso fraudulento o no autorizado a la Información de la Empresa.
5. Establecer e implementar controles idóneos para proteger la Información y las Bases de Datos contra pérdida, destrucción y falsificación de información de la Empresa.
6. Revisar y recibir las actualizaciones de seguridad o notificaciones de aplicación de parches de seguridad.
7. Realizar el borrado remoto de Información en dispositivos móviles en caso de pérdida o hurto.
8. Implementar el procedimiento de borrado seguro a los equipos informáticos devueltos por parte del empleado que termine su relación laboral con la Empresa.
9. Probar con regularidad los medios de respaldo para garantizar que sean confiables en situaciones de emergencia e informar al Oficial de Seguridad de la Información cuando el proceso de restauración haya generado errores y no termine exitosamente, explicando las razones de dicha conclusión.
10. Dar a conocer a los Usuarios información sobre buenas prácticas en materia de Seguridad de la Información y sobre nuevos tipos de Códigos Maliciosos o Amenazas con el fin de mitigar riesgos al interior de la Empresa.
11. Supervisar la efectividad de los mecanismos de seguridad física y control de acceso a los Centros de Datos.
12. Comunicar al Oficial de Seguridad de la Información las fallas en el procesamiento de la Información para que se tomen medidas correctivas.

Oficina de Tecnología Informática (“OTI”)

La OTI está compuesta por el Oficial de Seguridad de la Información y el Oficial de Sistemas, quienes adicional a sus roles individuales, trabajarán en conjunto con el fin de lograr los objetivos de las Políticas en materia de Seguridad de la Información. Dentro de la Empresa, la OTI tendrá los siguientes roles no obstante los demás que se puedan encontrar en el presente documento o en otros complementarios:

1. Instalar, actualizar y el asegurar el uso constante del software de detección de códigos maliciosos.
2. Asegurar que a las herramientas de software de detección de Códigos Maliciosos no se les puedan realizar cambios en la configuración ni ser deshabilitadas de los equipos, y deban ser actualizados permanentemente.
3. Desarrollar el plan interno de *backups* en el que se establezca el tipo de Información a que se le debe aplicar el *backup*, cuándo se aplica, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de Información.
4. Validar que los *backups* hayan sido ejecutados exitosamente. En el caso de que se encuentre una falla en la ejecución o en el resultado del *backup*, lo debe iniciar manualmente y registrar lo ocurrido y las medidas implementadas.

5. Instalar software o programas utilitarios, con previa revisión de las condiciones de licenciamiento.
6. Trabajar de manera conjunta cuando se detecte una Amenaza o algún Incidente de Seguridad. Deberá seguir los procedimientos incluidos en el Manual de Políticas y Procedimientos de ORAL X para seguir los pasos adecuados en estas situaciones.
7. Garantizar las medidas de seguridad adecuadas en todos los repositorios de Información y monitorear su idoneidad.
8. Llevar a cabo reuniones periódicas donde se garantice que los roles se complementen y estén alineados en el propósito común de la Seguridad de la Información.
9. Llevar a cabo el seguimiento, revisión y auditoría a los servicios que prestan los proveedores con el fin de fin de verificar el cumplimiento de los contratos y las obligaciones en materia de Confidencialidad y Seguridad de la Información.
10. Identificar los Usuarios a los que se le deben habilitar los accesos a los recursos informáticos y tecnológicos, relacionando los servicios que requieran y el tiempo de la habilitación, si ello es requerido.
11. Procurar que ORAL X. cuente con la infraestructura tecnológica adecuada para la plataforma que soporta el sistema Kubapp.
12. Responsable de mantener en operación la red inalámbrica bajo las condiciones de seguridad y Confidencialidad adecuadas.
13. Implementar los controles necesarios para asegurar el adecuado uso de la Intranet.
14. Dispondrá lo necesario para garantizar la protección de la información por accesos no autorizados o fraudulentos.
15. Velar por el uso adecuado de los dispositivos de la Empresa por parte de los empleados.

Coordinador de Talento Humano

El Coordinador de Talento Humano es el encargado de administrar la vida útil de los Datos Personales de los candidatos, empleados y ex empleados de la Empresa. Por lo anterior, dentro de ORAL X, tendrá los siguientes roles en materia de Seguridad de la Información, no obstante, los demás que se puedan encontrar en el presente documento o en otros complementarios:

1. Velar por el cumplimiento adecuado de la Política de Seguridad del Recurso Humano del Empleado incluida en la sección 5.3 de la presente Política.
2. Obtener de cada uno de los candidatos a procesos de selección autorización previa, expresa e informada para Tratar su Información Personal para la Finalidad relacionada con el proceso de selección. En caso de no poder obtener la mencionada autorización, deberá al menos poner en conocimiento de los Titulares (candidatos) un aviso de privacidad donde se establezca de manera clara la Finalidad del Tratamiento, la Política de Tratamiento de Datos Personales de la Empresa y los derechos del Titular, adicional a los demás requisitos de ley.
3. Obtener de cada uno de los empleados de la Empresa autorización previa, expresa e informada para Tratar su Información Personal para la Finalidad relacionada con la ejecución del contrato laboral y otras que apliquen como el uso de la imagen, el Tratamiento de Información Personal de familiares, entre otros.
4. Garantizar que los acuerdos de confidencialidad y no divulgación de la Información sean firmados por cada uno de los empleados a fin de proteger la información de la Empresa durante y después de la relación laboral.
5. Poner en conocimiento de los empleados la presente Política de Seguridad de la Información, la Política de Tratamiento de Datos y el Manual de Políticas y

Procedimientos de ORAL X y asegurarse de que los empleados acepten de manera expresa que conocen el contenido de los mismos y guardar prueba de dicha aceptación.
6. Comunicar a la OTI cuando se vaya a acabar una relación laboral para que se tomen en conjunto las medidas necesarias para garantizar la Seguridad de la Información.
7. Almacenar sólo la Información de ex empleados que sea necesaria para dar cumplimiento a obligaciones legales o judiciales.
8. Actualizar y depurar de manera periódica, y con supervisión del Oficial de Seguridad de la Información, las Bases de Datos de candidatos, empleados y ex empleados de ORAL X Cuando dicha actualización requiera de actualización en el RNBD, deberá comunicar tal situación al Oficial de la Información para que haga las actualizaciones necesarias en el registro.
9. Identificar y valorar la Información que requiere mayor protección para el cumplimiento de las normas por parte de la Empresa.
10. Apoyar en la adecuada implementación de procedimientos para custodiar la Información e Información Personal de ORAL X , para lo cual deberá trabajar en conjunto con el Oficial de Seguridad de la Información.
11. Mantenerse actualizado sobre las obligaciones en materia de Datos Personales y Seguridad de la Información.
12. Velar, en conjunto con la OTI, por el uso adecuado de los dispositivos de la Empresa por parte de los empleados.

Política de Seguridad para los Procesos Internos

Objetivo: definir de manera clara las políticas y procedimientos necesarios en cada uno de los procesos internos de la Empresa para garantizar la Seguridad de la Información. A continuación se hará una mención de los procesos más estructurales sin perjuicio de que el Oficial de Seguridad de la Información establezca e implemente unos adicionales que al ser documentados y socializados harán parte integral de este documento.
Estos lineamientos deben leerse en conjunto con la Política de Tratamiento de Datos Personales y el Manual de Políticas y Procedimientos de ORAL X

Proceso de relaciones con los empleados

Objetivo: asegurar la implementación de medidas de Seguridad de la Información en el proceso de contratación de los candidatos, empleados y ex empleados, así como de sus obligaciones antes, durante y después de la relación laboral. El Coordinador de Talento Humano y el Oficial de Seguridad de la Información serán responsables de su supervisión.

a. Control previo a asumir el empleo

Para llevar a cabo los procesos de selección de la Empresa, el Coordinador de Talento Humano debe Tratar la Información Personal de los candidatos para las Finalidades relacionadas con dicho proceso. Adicionalmente, durante la etapa de selección, el Coordinador del Talento Humano y la Dirección Administrativa directamente o a través del Oficial de Cumplimiento de la Empresa, deben verificar los antecedentes de todos los candidatos a un empleo en la empresa de acuerdo con las leyes, reglamentos y ética pertinentes (proceso de debida diligencia de SAGRILAFT).

Para tales efectos, ORAL X, obtendrá Autorización previa, expresa e informada por parte del candidato, Titular de los Datos Personales, previo a su Tratamiento. En caso de no poder obtener la mencionada Autorización, deberá al menos poner en conocimiento de los Titulares (candidatos) un aviso de privacidad donde se establezca de manera clara la Finalidad del Tratamiento, la Política de Tratamiento de Datos Personales de la Empresa y los derechos del Titular, adicional a los demás requisitos de ley.
Una vez se defina cuál es el candidato elegido en el proceso de selección, el Coordinador de Talento Humano deberá eliminar la Información Personal de los demás candidatos por darse por terminada la Finalidad del Tratamiento. El Oficial de Seguridad de la Información deberá supervisar que esto se lleve a cabo de manera adecuada.

b. Control durante la ejecución del empleo

Al momento de formalizar el contrato laboral, el empleado, de manera voluntaria deberá autorizar a ORAL X, para que lleve a cabo el Tratamiento de sus Datos Personales para las Finalidades necesarias para la ejecución del contrato. En la medida en que ORAL X sólo podrá Tratar los Datos Personales una vez cuente con Autorización previa, expresa e informada por parte de cada uno de los Titulares, en los casos en los que la Autorización no sea brindada por parte del Titular, ORAL X se verá en imposibilidad de ejecutar el contrato laboral lo cual debe ser puesto en conocimiento del Titular para que tome una decisión informada.
En caso de aceptar otorgar la Autorización, cada uno de los empleados de la Empresa firmarán la Autorización previa, expresa e informada para Tratar su Información Personal para la Finalidad relacionada con la ejecución del contrato laboral y otras que apliquen como el uso de la imagen, el Tratamiento de Información Personal de familiares, las Transmisiones o Transferencias de Información, entre otros.
Asimismo, los empleados deberán firmar un acuerdo de confidencialidad y no divulgación de la Información que incluye las obligaciones que como empleados deben cumplir para proteger la información de la Empresa durante y después de la relación laboral.
Por último, se deberá poner en conocimiento de los empleados la presente Política de Seguridad de la Información, la Política de Tratamiento de Datos y el Manual de Políticas y Procedimientos de ORAL X por lo que, al momento de la firma del contrato laboral, los empleados deberán adicionalmente aceptar de manera expresa que conocen el contenido de los documentos antes mencionados. El Coordinador de Talento Humano debe poner de presente estos documentos y asegurarse de que los empleados acepten que conocen el contenido de los mismos y guardará prueba de dicha aceptación.
Todos los empleados deberán recibir la capacitación y/o formación para la toma de conciencia apropiada en materia de Seguridad de la Información. Se implementarán evaluaciones periódicas del cumplimiento de las Políticas de Seguridad de la Información por parte de todos los empleados las cuales estarán a cargo del Oficial de Seguridad de la Información.
Adicional a las consecuencias contempladas en el contrato laboral y a las acciones aplicables por daños generados por la violación de las obligaciones de Seguridad de la Información y de Protección de Datos Personales a los empleados que incumplan y/o violen las Políticas de Seguridad de la Información de ORAL X , se les aplicará lo establecido en el Código sustantivo del trabajo, el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las reglamenten o complementen.

c. Control durante la terminación del contrato laboral

Al momento de una terminación del contrato laboral, el Coordinador de Talento Humano en conjunto con el Oficial de Sistemas, implementarán el procedimiento de borrado seguro a los equipos informáticos devueltos por parte del empleado que termine su relación laboral con la Empresa, con el fin de que la Información contenida no pueda ser recuperada posteriormente por quienes se desvinculan.

Al terminar su empleo, todos los empleados deberán devolver todos los activos de Información de propiedad de ORAL X , que estén y/o se encuentren a su cargo.

En el evento de cambio de labores de algún(nos) empleado(s) a otras áreas, éste(os) deben realizar la entrega de su puesto de trabajo al jefe inmediato. Igualmente, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de Información suministrados en el momento de su vinculación inicial y/o anterior.

Cuando se reubique a un empleado en otra área, se debe realizar la respectiva acta de entrega del activo que recibe y la validación del estado en el que se encuentra dicho activo. En el evento de que se trate de equipos portátiles y/o dispositivos móviles se instalará de nuevo el sistema operativo y demás programas básicos necesarios.

Con el fin de implementar las medidas necesarias a la terminación del contrato laboral el Coordinador de Talento Humano en conjunto con la OTI deberán, como mínimo:

1. Eliminarle (al exempleado) el acceso a los sistemas de información incluyendo el Sistema Kubapp y la Intranet así como el acceso a computadores y/o dispositivos móviles corporativos.
2. Eliminarle (al exempleado) el acceso a los Datos Personales de los sistemas de control de acceso del Sistema Kubapp y de la Intranet como todos los demás relevantes.
3. Realizar un inventario de devolución de equipos de ORAL X que estaban a cargo del empleado y sobre las condiciones del equipo al momento de la devolución.
4. Llevar a cabo una revisión técnica de los dispositivos objeto de devolución para asegurar que estén en condiciones operativas adecuadas y que se haya realizado el borrado seguro de datos. Esta revisión deberá documentarse y firmarse como parte del proceso de devolución.
5. Desactivar, si es aplicable, el carnet de identificación o cualquier medio de autenticación, que lo acredita como empleado de ORAL X y retiro inmediato del mismo.
6. Informar a los proveedores y demás personal con el que el empleado tenga contacto, indicándoles que esa persona ya no labora en ORAL X y estableciendo quién asumirá sus funciones o responsabilidades al interior de la Empresa.
7. Almacenar, al finalizar el proceso, sólo la Información de exempleados que sea necesaria para dar cumplimiento a obligaciones legales o judiciales.

Proceso en las relaciones con los proveedores, contratistas y terceros

Objetivo: establecer los requisitos de seguridad de la información pertinentes con cada proveedor, contratista y/o tercero que pueda tener acceso, procesar, almacenar, comunicar o en general Tratar Información de ORAL X La Dirección Administrativa y el Oficial de Seguridad de la Información serán responsables de su supervisión.

a. Control antes de la relación contractual

Cuando se obtenga de los proveedores, contratistas o terceros Información Personal, la Auxiliar Administrativa y/o el Área Contable deberán obtener autorización previa, expresa e informada por parte de los Titulares si llega a ser el caso y guardar prueba de ello por cada uno de los Titulares. Asimismo, deberán firmar un acuerdo de confidencialidad y no divulgación de la Información que incluye las obligaciones que como contratistas deben cumplir para proteger la información de la Empresa durante y después de la relación contractual.

Adicionalmente, se deberá poner en conocimiento de los proveedores, contratistas y/o terceros la presente Política de Seguridad de la Información, la Política de Tratamiento de Datos y el Manual de Políticas y Procedimientos de ORAL X por lo que, al momento de la firma del contrato, deberán adicionalmente aceptar de manera expresa que conocen el contenido de los documentos antes mencionados. El Área Contable debe poner de presente estos documentos y asegurarse de que los proveedores, contratistas y/o terceros acepten que conocen el contenido de los mismos y guardará prueba de dicha aceptación.

Por último, en los casos en los que haya flujo de Información Personal para llevar a cabo la finalidad del contrato, se deberá firmar un Contrato de Trasferencia o de Transmisión según sea aplicable conforme a la ley 1581 de 2012 y el decreto 1377 de 2013.

b. Control durante la relación contractual

Los líderes de los procesos al interior de la Empresa, únicamente pueden proporcionar a los proveedores, contratistas y/o terceros los accesos a la Información que sea estrictamente necesaria para cumplir el objeto del contrato suscrito, pero siempre que para ello se cuente con el visto bueno del Oficial de Seguridad de la Información y la autorización por parte de la Gerencia.

La OTI, con regularidad, debe hacer seguimiento, revisión y auditoria a los servicios que prestan los proveedores con el fin de fin de verificar el cumplimiento de los contratos y las obligaciones en materia de Confidencialidad y Seguridad de la Información.

La Gerencia gestionará los cambios de los servicios que le presten sus proveedores, contratistas y/o terceros (incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes), cada vez que la criticidad de la Información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos que así lo requieran y/o demanden.

Por regla general, ningún proveedor, contratista y/o tercero tendrá acceso directo a las Bases de Datos de ORAL X, a sus repositorios de información tales como el Sistema Kubapp, la Intranet o el Centro de Datos. Excepcionalmente, los proveedores, contratistas y/o terceros con autoridad para permitir el retiro directo de activos de Información deben estar claramente identificados y deben contar con el visto bueno del Oficial de Seguridad de la Información y la autorización por parte de la Gerencia.

c. Control posterior a la terminación de la relación contractual

Al terminar su contrato y/o acuerdo, todos los proveedores, contratistas y/o terceros, deberán devolver todos los activos de propiedad de ORAL X, que estén y/o se encuentren a su cargo. Esto incluye la Información que se les haya entregado en caso de ser aplicable.

Adicionalmente, deberán devolver a ORAL X los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación del servicio o la relación contractual.

En el caso excepcional en el que se le haya dado al contratista, proveedor y/o tercero acceso directo al Sistema Kubapp, la Intranet o el Centro de Datos, al momento de la terminación se seguirán las reglas de borrado equivalentes a las de los empleados.

Política de Uso Adecuado de la Información en Medios Digitales

5.3.1. Uso Adecuado de Dispositivos de la Empresa

Objetivo: dar lineamientos sobre el uso adecuado de los dispositivos de la Empresa. El Coordinador de Talento Humano y la OTI, son los responsables de su aplicación.

a) Lineamientos generales

Todos los empleados de ORAL X, cuentan con dispositivos entregados por la Empresa incluidos dispositivos móviles y/o computadores corporativos. Antes de entregar los mencionados dispositivos al empleado, el Coordinador de Talento Humano, en conjunto con la OTI, garantizarán que tales dispositivos cuenten con las medidas de Seguridad adecuadas. Asimismo, el Oficial se Sistemas garantizará que se hagan revisiones y actualizaciones de manera periódica (versiones actualizadas de software actualización de antivirus, entre otras).

Una vez obtengan los dispositivos, todos los empleados se comprometen a:

1. Hacer uso adecuado de la Información e Información personal contenida en los dispositivos.
2. Utilizar la Información a la que tienen acceso a través de estos dispositivos únicamente para las Finalidades autorizadas y relacionadas con el desarrollo de las labores y/o actividades que les han sido asignadas por ORAL X

3. Evitar almacenar videos, fotografías o información personal en los dispositivos corporativos.
4. Evitar utilizar canales de chat o grupos sociales como Facebook, X, Instagram, YouTube, canales de música, videos en la web, etc. en los dispositivos institucionales. Para efectos de situaciones puntuales, la Gerencia autorizará el uso de ciertas páginas de Internet.
5. Evitar utilizar sus dispositivos personales para acceder a los sistemas de ORAL X por lo que se limitarán a acceder a la información sólo a través de los dispositivos entregados y/o autorizados por ORAL X
6. Implementar un esquema de autenticación y desbloqueo del dispositivo como, por ejemplo, autenticación por contraseña o patrón de movimiento.
7. Evitar modificar las configuraciones de Seguridad de la Información, desinstalar el software provisto en los mismos o las restricciones que el sistema les imponga a través de la OTI.
8. Evitar la instalación de programas desde fuentes externas y/o de procedencia desconocida.
9. Evitar conectar los dispositivos corporativos por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
10. Evitar retirar los dispositivos fijos de las instalaciones de ORAL X , salvo autorización expresa de la Gerencia la cual deberá constar por escrito identificando la persona a cargo, la razón de la excepción y el tiempo por el cual será otorgado el permiso y los riesgos asociados a la autorización con sus respectivas recomendaciones para mitigarlos. El responsable del dispositivo deberá seguir las recomendaciones para disminuir los riesgos asociados al proceso de retiro, el medio de transporte y la ubicación del dispositivo en el sitio de destino más adecuado durante el tiempo que dure fuera de las instalaciones de la Empresa.
11. Seguir las mismas reglas de creación de contraseñas aplicables al Sistema Kubapp.
12. Tener configurado un protector de pantalla protegido con contraseña, el cual se debe activar después de un período de 15 minutos de inactividad. La reactivación del protector de pantalla debe exigir el ingreso de usuario y contraseña.
13. Cerrar (Log-Off), las aplicaciones o servicios de red cuando ya no se necesiten.
14. Localizar los dispositivos preferiblemente en ubicaciones físicas de modo que las pantallas no queden expuestas y puedan ser visualizadas por personas externas.
15. Bloquear la pantalla de sus computadoras al ausentarse de sus puestos y asegurarse de que no queden documentos físicos o medios de almacenamiento con Información Sensible en sus escritorios, almacenándolos en un lugar seguro.
16. Evitar el uso no autorizado de fotocopiadoras u otros dispositivos de reproducción, y se debe retirar y destruir de inmediato cualquier documento con Información Sensible de las impresoras, evitando su reutilización.
17. Evitar consumir alimentos o bebidas cerca de los equipos de cómputo, es necesario mantener el escritorio digital libre de accesos e íconos innecesarios.
18. Reportar a la OTI (al momento de conocer el hecho o máximo dentro de las 12 horas siguientes) en caso de robo o pérdida de un dispositivo institucional. Una vez hecho el reporte, la OTI delegará a quién deba realizar el borrado remoto de

la información almacenada en el dispositivo con el fin de evitar que la información quede expuesta a terceros no autorizados y seguir lo dispuesto en el Manual de Políticas y Procedimientos en materia de Incidentes de Seguridad.

La OTI, dispondrá lo necesario para garantizar la protección de la información por accesos no autorizados o fraudulentos. En caso de existir alguna falla, los requerimientos asociados a recursos tecnológicos, así como la solicitud de nuevos aplicativos o dispositivos deberán ser enviados a la OTI con la debida explicación. En los casos que se considere necesario, la OTI deberá involucrar a la Dirección Administrativa para poder resolver casos particulares.

Adicionalmente, la OTI, podrá borrar todos los datos de los dispositivos de forma remota, siempre y cuando exista una prueba que indique el uso indebido del dispositivo. También podrá eliminar la cuenta institucional de los dispositivos de forma remota, cuando se identifique el incumplimiento de cualquiera de las Políticas de Seguridad de la Información de ORAL X por parte del empleado o cuando finalice su relación laboral con la Empresa.

b) Manejo adecuado del correo electrónico institucional

El servicio de correo electrónico institucional es una herramienta para el intercambio de información exclusivamente laboral. El único servicio de correo electrónico autorizado para el manejo de la información institucional de ORAL X cuenta con el dominio @oralx.co, salvo casos específicos autorizados por la Gerencia.

Aquellos que cuenten con un correo electrónico de ORAL X deberán:

1. Seguir las mismas reglas de creación de contraseñas aplicables al Sistema Kubapp.
2. Utilizar las cuentas de correo institucional para el uso exclusivo de las funciones y/u obligaciones de los empleados y nunca para fines personales.
3. Utilizar las cuentas de correo institucional bajo los criterios de racionalidad, respeto, Protección de Datos Personales, Confidencialidad y Seguridad de la Información. Los empleados de ORAL X, son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.
4. Implementar medidas de protección mediante autenticación multifactor de manera que no solo se use una contraseña para ingresar al correo, sino también un segundo factor como una aplicación de autenticación o un código enviado al móvil para garantizar mayor seguridad.
5. Notificar inmediatamente a la OTI en caso de que detecte un Incidente de Seguridad relacionado con el correo, como el acceso no autorizado o fraudulento, la recepción de correos sospechosos o la pérdida de Información.
6. Evitar enviar mensajes de correo electrónico con contenidos que comprometan el buen nombre de ORAL X, instituciones o personas. Por lo tanto, se prohíbe usar el correo institucional para la propagación de correos con mensajes cadena, mensajes publicitarios, imágenes o videos que contengan contenidos ofensivos, material sexual, de intimidación, con contenidos ilegales o de discriminación de

género, nacionalidad, religión, raza, orientación política o discapacidad.

7. Enviar correos masivos únicamente cuando sea necesario y se haya obtenido Autorización previa, expresa e informada por parte del Titular del correo electrónico al cual está siendo enviado el mensaje. Adicionalmente, en esos casos, es necesario proteger los correos de la cadena con la opción “copia oculta” para evitar que todos los receptores de la información obtengan los correos en copia de manera masiva. En ningún caso está permitido compartir contactos o listas de distribución de ORAL X, con personal externo.
8. Evitar la distribución de software o contenidos que violen la propiedad intelectual o derechos de autor, así como las leyes en materia de Datos Personales.
9. Utilizar listas de distribución internas sólo para cumplir los fines de comunicación e información interna, más no para fines diferentes a los del cumplimiento de los objetivos de ORAL X
10. Evitar alterar la información existente en un correo electrónico cuando en una respuesta se incluya el mensaje original.
11. Evitar imprimir correos electrónicos salvo que sea estrictamente necesario caso en el cual las impresiones se deben almacenar de forma segura. Se evitará en lo posible reproducir Bases de Datos de manera digital y física cuando ello no sea estrictamente necesario.
12. Incluir en cada correo electrónico el logo de ORAL X, y la firma oficializada ante y por la Empresa. Cuando la información allí contenida sea información confidencial se deberá incluir en el correo una leyenda que así lo indique.
13. Usar antivirus de la Empresa para detectar adjuntos que contengan información maliciosa.
14. Llevar a cabo una administración periódica de su cuenta para evitar bloqueos por factores como el llenado de su buzón.
15. Tener activada la opción de correo no deseado para evitar correos que pueden contener links o información fraudulenta.

c) Cifrado de la información contenida en los dispositivos

La OTI deberá proteger la Confidencialidad, Autenticidad e Integridad de la información de ORAL X , por medio del uso adecuado de controles criptográficos y de cifrado que se implementan en el disco duro de los computadores institucionales. Para llevar a cabo lo anterior, la OTI deberá:

1. Promover mecanismos de cifrado para la protección de Información e Información Personal en los dispositivos institucionales.
2. Administrar la gestión de claves de cifrado, lo cual incluye su generación, distribución y revocación de las mismas.
3. Proteger físicamente los equipos usados para generar, almacenar y archivar las claves de cifrado.
4. Revocar las claves de cifrado; por ejemplo, cuando la seguridad de las claves haya estado comprometida, o cuando un usuario deja la empresa (en cuyo caso las claves también se deberán eliminar).
5. Mantener un registro de las operaciones de gestión de claves de cifrado (claves generadas, distribuidas y revocadas), al igual que del propietario de las claves y del tiempo de validez.

5.3.2. Uso Adecuado del Sistema Kubapp

Objetivo: dar lineamientos sobre el uso adecuado del Sistema Kubapp, aplicación utilizada por ORAL X para manejar, configurar, administrar y almacenar de manera centralizada y automatizada su Información e Información Personal. El Sistema Kubapp integra el control de inventario, facturación, compras, cartera, cuentas por pagar, caja, entre otros. La OTI, en conjunto con la Gerencia, serán los encargados del buen funcionamiento de la utilización de la plataforma.

a) Generalidades

Los empleados de ORAL X, Usuarios del Sistema Kubapp, utilizarán este sistema como un recurso de consulta de los documentos internos. El acceso a Kubapp debe estar limitado según el rol de cada usuario. Sólo los Usuarios autorizados podrán acceder a Información.
Los Usuarios deberán:

1. Acceder únicamente a la Información para la cual esté autorizado.
2. Velar porque la Información contenida en el Sistema Kubapp esté actualizada por lo que deberá trabajar de la mano con la OTI en caso de que se requiera una actualización.
3. Evitar compartir Información del Sistema Kubapp con terceros.
4. Evitar usar la identidad de otro Usuario.

b) Control de acceso

Cuando se autoriza a un Usuario a acceder al Sistema Kubapp, se seguirá un procedimiento formal para la creación y aprobación de cuentas de Usuario.
Cada Usuario debe disponer de una identificación única (ID) que permita determinar los responsables de una acción operativa. Sólo se permiten identificadores de grupo cuando se justifican por razones operativas y bajo aprobación por parte de la Gerencia y del Oficial de Seguridad de la Información. Por ningún motivo se deben crear cuentas de usuario genéricas.
Se debe mantener un registro formal de todos los Usuarios autorizados y de sus niveles de acceso asignados y se debe verificar dicho registro periódicamente.
Adicionalmente, se debe implementar un Control de Acceso Basado en Roles, donde los permisos se asignen según la clasificación de la Información. Esto implica que los Usuarios sólo tendrán acceso a los datos y aplicaciones necesarios para su rol específico dentro de la Empresa.
La Coordinación de Talento Humano y la OTI, deberán verificar cada seis (6) meses que los niveles de acceso asignados a los Usuarios sean apropiados de acuerdo al propósito del negocio. En el caso de que un activo de Información aumente su nivel de criticidad o que contenga Información Personal Sensible, se deberá realizar una revisión de los Usuarios que acceden a él y de los riegos asociados.
En caso de que un usuario sea retirado o reasignado en sus funciones, el coordinador de Talento Humano debe informarlo a la OTI, vía correo electrónico para hacer el bloqueo del Usuario de manera adecuada.

c) Contraseñas

Cada Usuario tendrá una contraseña de acceso al Sistema Kubapp a la que sólo tendrán acceso el Usuario y la OTI. En el momento de la asignación de una contraseña a un Usuario o a un grupo de usuarios, la OTI, informará a aquellos sobre el carácter confidencial de ésta y el Usuario deberá:

1. Asumir responsabilidad por el uso de las contraseñas de acceso que se les asignen para la utilización del Sistema Kubapp y demás dispositivos institucionales.
2. Cambiar la contraseña cuando ésta haya sido por defecto asociada a un software o sistema de información.
3. Seleccionar contraseñas con un mínimo de ocho (8) caracteres, que sean alfanuméricas (que contenga números, mayúsculas y minúsculas) y que contengan caracteres especiales (#$%@/).
4. Evitar crear contraseñas que tengan relación con el nombre propio, familiares, cargo de trabajo, etc.
5. Cambiar la contraseña siempre que haya indicio de puesta en peligro del sistema o a intervalos regulares, evitando la reutilización de contraseñas antiguas.
6. Evitar almacenar las contraseñas en un computador con un formato no cifrado.
7. Evitar mantener registros de las contraseñas (hojas de papel, archivos digitales, etc.), a menos de que sea un método de almacenamiento aprobado por el Oficial de Seguridad de la Información.
8. Evitar almacenar las contraseñas en un proceso de registro automatizado (plugin, extensión, macro, etc.).
9. Evitar compartir las contraseñas con terceros.
10. Evitar usar las mismas contraseñas para propósitos del negocio y para propósitos personales.
11. Cambiar la contraseña, como mínimo, cada 6 meses y aquella debe ser distinta de las que utilizó las últimas 5 veces.
12. Desactivar la opción de autoguardado de contraseñas en el Sistema y otros navegadores web y dispositivos institucionales.
13. Utilizar un proceso de recuperación de contraseña que incluya la verificación de identidad mediante preguntas de seguridad preestablecidas previamente registrado y validado cuando se le olvide la contraseña.

d) Mantenimiento, actualización y monitoreo

La OTI debe implementar un sistema de monitoreo y registro de actividades en el Sistema Kubapp para asegurar que no se acceda ni modifique Información de manera no autorizada. Cualquier actividad sospechosa o anormal deberá ser reportada inmediatamente.
Adicionalmente, la OTI deberá deputar constantemente las Bases de Datos y asegurarse de que los datos allí contenidos están actualizados, legitimados y sean exactos.

5.3.3. Uso adecuado del Internet, las Redes Inalámbricas y el Servicio de Nube

Objetivo: dar lineamientos al momento de usar herramientas como el Internet, las redes inalámbricas y el servicio de nube.

a) Internet

Todos los accesos a internet deben ser realizados a través de los canales de acceso provistos por la Gerencia, con asistencia de la OTI, la cual sólo dará autorización de uso a los servicios de Internet que puedan ofrecerse de manera segura.
El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades laborales y/o comerciales de ORAL X
No está permitida la conexión a dominios de Internet que generen tráfico de broadcast (audio o video) por fuera de los dominios institucionales de ORAL X
No está permitido acceder a páginas clasificadas con contenido pornográfico o no permitidas.
No se debe instalar software que permita acceder a páginas o servicios no autorizados como los VPNs.
Está prohibido compartir archivos o enlaces que provengan de fuentes no confiables o que no hayan sido previamente escaneados en busca de malware. Esto incluye el reenvío de correos electrónicos con enlaces o archivos adjuntos no verificados.

b) Redes inalámbricas

Se debe contar tanto con mecanismos de control de acceso lógico (permisos que se les da a los Usuarios para ingresar a la red) para salvaguardar la Confidencialidad e Integridad de la Información e Información Personal que pasa sobre redes inalámbricas, como con métodos de autenticación que eviten accesos fraudulentos o no autorizados.
Para las conexiones a redes inalámbricas, sólo se deben permitir esquemas de Seguridad que provean Confidencialidad de la Información e Información Personal del Usuario transferida sobre medios inalámbricos y autenticación para dispositivos compatibles con el estándar IEEE 802.11 de seguridad que son válidos y proveen Confidencialidad y autenticación sobre medios inalámbricos para dispositivos IEEE 802.11: WPA-PSK, WPA2-PSK y 802.1X. Bajo ninguna circunstancia se debe usar WEP.
Los Usuarios se obligan a hacer uso productivo y seguro de la red inalámbrica y a usarla bajo los estándares de diligencia, por lo que deben evitar hacer uso de redes inalámbricas de uso público.
Quienes tengan asignados dispositivos móviles institucionales, deben desactivar las redes inalámbricas como WIFI, Bluetooth o infrarrojos, que tengan instaladas en los mismos.

c) Servicio de nube

No está permitido almacenar Información de ORAL X, en servicios de alojamiento de archivos multiplataforma en la nube (Dropbox, Onedrive, Box, Bitcasa, Mesa, icloud, entre otros o similares) que no hayan sido autorizados por la Gerencia de manera expresa.

5.4. Política de Seguridad Física y del Entorno

Objetivo: dar lineamientos para proteger las áreas físicas que contienen Centros de Datos con Información y/o Información Personal de ORAL X así como las Bases de Datos físicas con las que cuenta la Empresa.

5.4.1. Medidas de Seguridad del Centro de Datos

Objetivo: establecer los lineamientos para prevenir el acceso físico no autorizado o fraudulento, el daño y la interferencia a la Información y a las instalaciones de la Empresa donde se encuentran el Centro de Datos.

a) Generalidades

La Gerencia proveerá tanto las condiciones físicas y ambientales para la debida protección y correcta operación del Centro de Datos, como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas necesarios para la protección de la Información.
Las puertas de acceso al Centro de Datos deben permanecer siempre cerradas y aseguradas y con control de acceso adecuado.
El ingreso a las instalaciones de ORAL X , debe estar restringido únicamente al personal autorizado. Por lo tanto, el ingreso de un tercero o visitante a un Centro de Datos debe ser autorizado previamente por la Gerencia de manera expresa.
Los privilegios de acceso físico al Centro de Datos de las personal autorizadas deben ser eliminados a la terminación de la vinculación laboral o contractual, o por alguna otra novedad.
Cualquier movimiento dentro del Centro de Datos debe ser autorizado por la Gerencia.

b) Seguridad perimetral y CCTV

Todas las áreas de la oficina que tienen Bases de Datos deben ser físicamente seguras (es decir, no deben existir brechas y/o espacios en el perímetro y/o áreas donde fácilmente pueda ocurrir una intrusión).
En los sitios que contengan equipos y/o servicios de Tratamiento de Información e Información Personal se deben implementar mecanismos robustos físicamente (por ejemplo, cerraduras, barras, alarmas, sistemas de lectores de tarjeta, muros, puntos de acceso con vigilancia humana) aplicables para prevenir el acceso no autorizado o fraudulento. Las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión.
Todas las salidas de ORAL X, deben contar con alarma, y deben funcionar de manera segura.
En lo posible, se debe tener un sistema de vigilancia que permita la detección de intrusos en las instalaciones de la Empresa.
Con el propósito de supervisar y registrar las actividades de posibles intrusos, identificar elementos y cualquier tipo de circunstancia que resultase anormal, ORAL X, en lo posible, deberá implementar un Circuito Cerrado de Televisión (CCTV), cuya administración estará a cargo de la Dirección Administrativa. Las grabaciones realizadas a través del CCTV, deben ser informadas a todas las personas, incluyendo el propósito, responsabilidades y derechos frente

a las mismas, de acuerdo con la legislación vigente en materia de protección de datos personales.
La administración de las grabaciones obtenidas a través del CCTV, serán realizadas de acuerdo con lo establecido en el documento denominado “Procedimiento servicios administrativos”.
Con el fin de cumplir con las normas en materia de protección de datos, ORAL X deberá poner un aviso de privacidad de manera visible en sus oficinas con el fin de que las personas al interior de la oficina tengan claro que están siendo grabadas. El aviso deberá contar con los requisitos exigidos por ley.

c) Pólizas de seguros

El Oficial de Seguridad de la Información debe hacer una revisión de las pólizas de seguros asociadas a los activos de la Empresa (por ejemplo: hardware) y la cobertura de estas desde el momento en que el activo sale de las instalaciones de ORAL X
Los seguros deben considerar el cubrimiento mínimo de los costos de reposición de los recursos informáticos, costos de interrupción del negocio, el rembolso a la Empresa por costos en la restauración de las operaciones y pérdidas de ganancias asociadas. (A más tardar la segunda semana del mes de enero y la primera semana del mes de julio, la OTI revisará la correspondiente la actualización de los equipos y de sus precios).
Se debe considerar específicamente la cobertura en los tiempos de traslado del activo hasta las instalaciones donde éste permanecerá.
En caso de que una o varias pólizas de seguros no tengan cobertura por fuera de las instalaciones de ORAL X , se deberá validar la posibilidad de aceptación del riesgo.

5.5. Políticas Técnicas para Seguridad de Equipos

Objetivo: establecer mecanismos técnicos para reducir los riesgos de acceso no autorizado o fraudulento, pérdida y daño de información durante y por fuera de las horas laborales normales.
El Oficial de Sistemas estará a cargo de su implementación y el Oficial de Seguridad de la Información hará el monitoreo respectivo.

5.5.1. Control de código malicioso

Objetivo: proporcionar los lineamientos para implementar controles de detección, prevención y recuperación, para la protección de la Integridad de la Información y de las plataformas tecnológicas de ORAL X frente a Códigos Maliciosos.
Toda la infraestructura tecnológica y de procesamiento de Información y comunicaciones debe estar protegida mediante herramientas y software de seguridad para prevenir el ingreso de Códigos Maliciosos en la red interna de la Empresa.
La OTI debe disponer de herramientas de detección de Códigos Maliciosos como antivirus, antimalware, antispam y antispyware, manteniéndolas siempre actualizadas con las últimas definiciones del fabricante.

El software de detección de Códigos Maliciosos debe configurarse para realizar las siguientes verificaciones:

1. Examinar archivos en medios ópticos (CDs, DVDs), discos duros, memorias USB y archivos obtenidos de redes antes de su uso.
2. Analizar archivos adjuntos y descargas de correo electrónico para detectar Códigos Maliciosos antes de su uso.
3. Comprobar los códigos de las páginas web para detectar posibles Amenazas.
4. Verificar la presencia de Códigos Maliciosos en archivos destinados a ser enviados a un servidor, correo o equipo en la red.

En caso de sospecha de infección por Código Malicioso, se debe seguir el procedimiento de Gestión de Incidentes incluido en el Manual de Políticas y Procedimientos.
Todos los empleados y Encargados del Tratamiento tienen la responsabilidad de reportar cualquier incidente de infección de virus a la OTI.
Todos los sistemas operativos y aplicaciones deben tener instalados los parches y actualizaciones de Seguridad más recientes para bloquear Vulnerabilidades conocidas.
El Oficial de Seguridad de la Información y el Oficial de Sistemas son responsables de revisar y recibir actualizaciones de Seguridad y notificaciones sobre la aplicación de parches de Seguridad de la Información.
Todo programa de código fuente de los sistemas de Información y desarrollos de software de ORAL X debe ser examinado y aprobado por la OTI antes de su implementación en producción.

5.5.2. *Backups* o Respaldos de Información

Objetivo: establecer los lineamientos para mitigar el riesgo de pérdida de la Información definiendo la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información, software y sistemas.
La OTI, en conjunto con la Gerencia, definirán los casos en los que en necesario hacer *backups* o copias de respaldo de información. Todas las copias de respaldo deben registrarse en el "Formato de registro de Backups de la Información," detallando tipo, periodicidad, fecha de creación y periodo de retención. La generación de respaldos debe basarse en análisis de riesgos de la Información en ORAL X
Para sistemas críticos, los respaldos deben incluir todos los datos necesarios para la recuperación completa en caso de desastre.
La OTI es responsable del almacenamiento seguro de las copias.
Los respaldos se deben almacenar en una ubicación remota segura, con protección física y ambiental; por ejemplo, un segundo servidor o en la nube.
Se debe llevar un registro del transporte de los respaldos entre las instalaciones de ORAL X y el sitio de respaldo externo.
Los administradores de sistemas no deben almacenar información en particiones asignadas al sistema operativo o aplicativos.

Las copias de respaldo deben almacenarse en medios duraderos, como cintas o discos externos, con una durabilidad mínima de 12 meses. Los respaldos deben estar protegidos mediante cifrado.
Una vez vencido el periodo de retención, los medios de almacenamiento deben eliminarse.
El acceso a registros de ubicación y contenido de los medios de respaldo es restringido y autorizado solo por el Oficial de Seguridad de la Información.
Los medios deben etiquetarse adecuadamente: carpeta, tipo de backup, fecha de ejecución, y consecutivo.
Cada 30 días, la OTI realizará una restauración aleatoria para verificar la consistencia e integridad de los datos respaldados.
Cada *backup* se realizará sólo si es necesario, y cada duplicado llevará un número de radicación para asegurar el seguimiento y Seguridad de la Información.

5.5.3. Registro de Eventos y Seguimiento

Objetivo: definir el registro de Eventos y la realización de monitoreo sobre los registros. El Oficial de Seguridad de la Información estará a cargos de dichos registros.
Para efectos de llevar un registro de Eventos de manera adecuada, el Oficial de Seguridad de la Información debe:

1. Crear un mecanismo de radicados de cada uno de los registros.
2. Generar registros de auditoría de todos los Eventos relacionados con la Seguridad de la Información.
3. Sincronizar los relojes de los todos los sistemas con una única fuente de referencia de tiempo como la hora legal colombiana (http://horalegal.inm.gov.co/), para asegurar la exactitud de todos los registros de auditoría, que pueden ser necesarios para investigaciones o como evidencia en procesos legales o en asuntos disciplinarios.
4. Comunicar al Oficial de Sistemas y a la Gerencia cualquier falla en el Tratamiento de la Información para que se tomen las medidas correctivas necesarias.
5. Monitorear y revisar, junto con el Oficial de Sistemas, los registros de auditoría de la plataforma tecnológica y los sistemas de Información, identificando brechas de Seguridad y otros Eventos relevantes.
6. Registrar todos los Eventos de seguridad importantes en un log de Eventos para cualquier servidor que maneje información confidencial, incluyendo:

    - Errores de autenticación.
    - Modificaciones de datos.
    - Utilización de usuarios privilegiados.
    - Cambios en la configuración de acceso a archivos.
    - Modificaciones en los programas o el sistema operativo.
    - Cambios en los privilegios o permisos de usuarios.
    - Uso de cualquier función privilegiada del sistema.

7. Salvaguardar los registros de auditoría que se generen en la plataforma tecnológica y los sistemas de información, para certificar la Integridad y

Disponibilidad de los mismos. Los registros sólo deben ser accedidos por personal autorizado.

8. Por reportes recibidos de algún(os) funcionario(s) de la empresa, debe registrar todos los errores y fallas en el procesamiento de información o en sistemas de comunicación, incluyendo:

    - Nombre de la persona que reporta la falla.
    - Hora y fecha de ocurrencia.
    - Descripción del error o problema.
    - Responsable de solucionar el problema.
    - Descripción de la respuesta inicial.
    - Descripción de la solución aplicada.
    - Hora y fecha de la resolución del problema.

En caso de ser notificado o darse cuenta de la ocurrencia de un Incidente de Seguridad, el Oficial de Seguridad de la Información deberá reportar tal situación a la SIC a través del RNBD conforme a lo dispuesto en el Manual de Políticas y Procedimientos de ORAL X.
Los logs (bitácoras) de seguridad deben ser almacenados por un periodo mínimo de tres (3) meses. El acceso a dichos logs debe ser permitido sólo a personal autorizado por el Oficial de Seguridad de la Información. En la medida de lo posible, los logs deben ser almacenados en medios de sólo lectura.

5.5.4. Gestión de Vulnerabilidades Técnicas

Objetivo: dar lineamientos para evaluar la exposición de ORAL X, a las Vulnerabilidades técnicas de información. La OTI es la encargada de la gestión de Vulnerabilidades y deberá:

1. Definir y establecer los roles y responsabilidades en la gestión de Vulnerabilidades técnicas y de seguridad de las plataformas tecnológicas.
2. Identificar y evaluar Vulnerabilidades técnicas y de seguridad, definiendo las herramientas y servicios necesarios para su detección.
3. Ejecutar un escaneo trimestral de Vulnerabilidades técnicas y de seguridad en las plataformas tecnológicas.
4. Verificar y realizar seguimiento para corregir las Vulnerabilidades identificadas, asegurando la protección de la infraestructura.
5. Documentar e informar los hallazgos y acciones tomadas para mitigar riesgos, y reportar incidentes a la SIC según sea necesario.
6. Tomar acciones urgentes para tratar Vulnerabilidades según los procedimientos de gestión de cambios o respuesta a incidentes de seguridad.

5.5.5. Gestión de seguridad en las redes

Objetivo: establecer mecanismos de control para la protección de la información en las redes de la Empresa lo que incluye redes internas como la Intranet y puntos de red físicos. El Oficial de Sistemas será el encargado de implementar las medidas y el Oficial de Seguridad de la Información será el encargado de su supervisión.

Los Usuarios de la red interna no pueden realizar acciones exclusivas de los administradores de red.
Tanto los empleados como los contratistas necesitan aprobación expresa de la OTI antes de instalar o configurar equipos y conexiones en la red.
Los Oficiales de Seguridad de la Información y de Sistemas determinan los puntos de acceso a la red, el procedimiento de autorización y los controles de protección de la red. Los servicios en los sistemas deben justificarse de acuerdo con las necesidades de la empresa, y los riesgos asociados deben resolverse antes de su implementación.
Los Oficiales de Seguridad de la Información y de Sistemas son responsables de proteger la Confidencialidad del direccionamiento y enrutamiento de redes. Por lo tanto, deben instalar sistemas de protección en la red, como firewalls y sistemas de detección de intrusos, y asegurarse de que los proveedores de red implementen mecanismos de seguridad.
Las redes inalámbricas deben estar separadas de la red principal para reducir riesgos, con control de acceso y autenticación segura. La separación de redes debe considerarse según los niveles de seguridad y tráfico, basándose en el tipo de información almacenada en cada red.
Las redes y servicios deben dividirse en dominios lógicos de red, cada uno con un perímetro de seguridad definido y aprobado por el Oficial de Seguridad de la Información.

5.5.6. Conexión remota por medio de Red Privada Virtual (VPN)

Objetivo: dar lineamientos sobre el acceso remoto bajo las condiciones de Seguridad adecuadas. El Oficial de Sistemas será el encargado de implementar las medidas y el Oficial de Seguridad de la Información será el encargado de su supervisión.
Por regla general, la Empresa no tiene la modalidad de teletrabajo, por lo que sus empleados trabajan en las instalaciones de la Empresa. Sin embargo, en caso de requerirse acceso remoto a las Bases de Datos y sistemas de información de la Empresa, se deberá pedir autorización expresa a la Gerencia y se deberán seguir las siguientes reglas:
El Oficial de Sistemas, debe garantizar que la conexión remota a la red interna de ORAL X, se realice a través de una conexión VPN SSL, suministrada por la Empresa. Asimismo, debe establecer métodos apropiados de autenticación para los Usuarios que utilicen accesos remotos.
Toda solicitud de creación de VPN, debe ser realizada en los formatos de Seguridad que más se adecuen a la red, los cuales deben ser aprobados por el jefe inmediato, que tenga como mínimo cargo de Dirección del grupo de trabajo del funcionario, o por el supervisor del contrato, para el caso de los contratistas.
Al establecer conexiones VPN haciendo uso de equipos ajenos a la empresa, los Usuarios entienden y aceptan que sus equipos de cómputo son una extensión de la red de datos de ORAL X, y por esa razón deben cumplir con las mismas políticas que aplican para los equipos de propiedad de la Empresa.
Es responsabilidad de los Usuarios que utilizan los servicios de VPN de ORAL X, asegurar que personas no autorizadas, no accedan a las redes de datos internas de la empresa.

Si la VPN no se ha utilizado, en al menos los últimos 90 días, ésta será eliminada. Pasado ese tiempo, en caso de requerirse nuevamente, debe surtirse de nuevo todo el proceso para la creación de la VPN, incluyendo el diligenciamiento del formato respectivo.

5.5.7. Borrado Seguro

Objetivo: prevenir el robo de la información de los activos de información que se dan de baja o van a ser utilizados por otro empleado en ORAL X. El Oficial de Seguridad de la Información y el de Sistemas, son los encargados de aprobar la herramienta de software más adecuada para escanear el medio de almacenamiento y ejecutar un borrado seguro.
La OTI es responsable de ejecutar el borrado seguro en los medios de almacenamiento y verificar que los datos no puedan ser recuperados, usando herramientas de recuperación para confirmación.
Para llevar a cabo el borrado de manera adecuada, el Oficial de Sistemas debe aprobar el software adecuado para el escaneo y borrado seguro de datos en dispositivos de ORAL X
La OTI debe notificar a la Gerencia, cuando se deba destruir físicamente un medio de almacenamiento que compromete la seguridad. Los activos físicos en mal estado con Información Sensible deben pasar por un análisis de riesgos para decidir si es mejor eliminarlos o repararlos.
Si no se puede realizar el borrado seguro, se debe considerar la destrucción del medio de almacenamiento.
En caso de pérdida o robo de dispositivos móviles institucionales, el Oficial de Sistemas, con aprobación del Oficial de Seguridad de la Información, debe realizar el borrado remoto para proteger la Información.
Los Oficiales de Seguridad y de Sistemas deben realizar pruebas post-borrado para asegurar que el proceso cumpla con los estándares de borrado seguro.
El borrado de Información Personal sólo se realizará una vez cumplida la Finalidad del Tratamiento, con Autorización del Titular o cuando se presente un Incidente de Seguridad.

5.6. Otros Requisitos Legales

Objetivo: evitar el incumplimiento de las obligaciones legales, estatutarias y de reglamentación relacionadas con la Seguridad de la Información y de cualquier requisito de seguridad.

5.6.1. Derechos de propiedad intelectual

Objetivo: dar los lineamientos para proteger adecuadamente la propiedad intelectual de la Empresa y de terceros (derechos de autor de software o de documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros).
No está permitido usar software no autorizado o duplicado sin licencia. Todo software en los equipos de ORAL X debe estar autorizado, adquirido legalmente y cumplir con los requisitos de licencia adecuados. La Empresa retirará el software cuando el propietario lo solicite, venza la licencia, o se termine el contrato con el proveedor.

Solo se debe usar software instalado siguiendo el procedimiento oficial, proveniente de fuentes confiables. Los Oficiales de Seguridad de la Información y de Sistemas, implementarán restricciones para la instalación de programas en los equipos y mantendrán un inventario de todo el software autorizado, con controles periódicos para detectar productos sin licencia. Además, ORAL X debe mantener un inventario corporativo de licencias para gestionar el control y la administración de software.
Todo material producido por empleados o contratistas durante sus labores pertenece exclusivamente a ORAL X, lo cual debe estipularse en los contratos. El Oficial de Seguridad de la Información también debe controlar que no se excedan los límites de usuarios en las licencias.
Por último, está prohibido copiar, duplicar o convertir materiales protegidos por derechos de autor sin autorización o más allá de lo permitido por la ley.

5.6.2. Privacidad y protección de información de datos personales

Objetivo: asegurar la privacidad y la protección de la información de datos personales, tal como se exige en la ley y en la reglamentación pertinentes, cuando ello sea aplicable.

ORAL X, se encuentra en pleno cumplimiento de la ley 1581 de 2012, el decreto 1377 de 2013 y las normas que las modifiquen y/o complementen. Adicionalmente la empresa cuenta con una Política de Tratamiento de Datos Personales y un Manual de Políticas y Procedimientos que deben ser consultados en conjunto con la presente Política de Seguridad.

5.7. Revisiones de Seguridad de la Información

Objetivo: establecer las normas que garanticen que la Seguridad de la Información se implemente y opere de acuerdo con las políticas y procedimientos empresariales.

Los líderes de los procesos de ORAL X, deben apoyar las revisiones del cumplimiento de los sistemas con las políticas, normas y procedimientos de seguridad apropiados y cualquier otro requerimiento de seguridad.

El Oficial de Seguridad de la Información, realizará acciones de verificación del cumplimiento de la Presente Política de Seguridad de la Información.

Cuando lo considere necesario, el Oficial de Seguridad de la Información en conjunto con la Gerencia, deberá actualizar la presente Política de Seguridad de la Información y dar a conocer la versión más reciente a todos sus accionistas, directivos, empleados, proveedores, contratistas y terceros.

Última actualización: 15 de enero de 2025.