MARCO DE POLÍTICAS DEL SGSI

1. Política SGSI

INTEGRA WEB, como organización proveedora de servicios de desarrollo de software y de Software como servicio, tiene un compromiso decidido hacia la calidad de su producto y la seguridad de la información propia y de terceros que se la hayan confiado, incluyendo los de carácter personal, deber que incluye al personal que actúa en nombre de la empresa, así como toda parte interesada que pueda tener acceso a dicha información.

El Sistema de gestión Integral en la organización está basada en la gestión de riesgos y su arquitectura de control la cual incluye medidas preventivas y reactivas de la organización y de los sistemas tecnológicos para proteger así la información en aras de lograr los objetivos de negocio mientras mantiene su confidencialidad, disponibilidad e integridad.

Nuestro compromiso reúne la gestión del cumplimiento y de la conformidad sobre los requisitos aplicables, tanto del ordenamiento jurídico pertinente, como contractual y técnico, haciendo especial énfasis en los aspectos de privacidad, transparencia y nivel de servicio, así como de la protección adecuada de información de carácter reservado.

Para asegurar la continua pertinencia del Sistema de Gestión Integral frente a posibles cambios en el contexto, especialmente en partes interesadas, requisitos aplicables, y la dinámica tecnológica y de mercado, asumimos el deber de mantener y mejorar de forma continua el Sistema de Gestión Integral y riesgos asociados.

2. Política para los dispositivos móviles

INTEGRA WEB, para la gestión integral en relación con su alcance respecto de los dispositivos móviles, ha establecido las siguientes directrices considerando los requisitos aplicables conforme a lo declarado en la política general integral y bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

ELEMENTO DEL ALCANCE	Procesamiento	Consulta	Almacenaje	
a. Prestación servicios de gestión de la información y sistemas de información (Software como servicios)	Permitido/in situ + offsite		Permitido con inspección	Portátiles
	No permitido		No permitido	iPad/Tablet
	Permitido/in situ		No permitido	Smartphone
	No permitido		No permitido	HDD externo
b. Administración delegada de infraestructura tecnológica, de hardware y de software, propia y/o de terceros	Permitido/in situ + offsite		Permitido con inspección	Portátiles
	No permitido		No permitido	iPad/Tablet
	No permitido		No permitido	Smartphone
	No permitido		No permitido	HDD externo
c. Ingeniería de software	Permitido/in situ + offsite		No permitido	Portátiles
	Permitido/in situ + offsite		No permitido	iPad/Tablet
	Permitido/in situ + offsite		No permitido	Smartphone
	No permitido		No permitido	HDD externo

1. Los dispositivos móviles autorizados para contener información de la compañía deben estar registrados en el inventario de activos de información.
2. Los celulares deben contar con clave y bloqueo automático.
3. Existe un listado de dispositivos móviles corporativos autorizados para ser retirados de la compañía.
4. No modificar las configuraciones de seguridad, software o hardware de los dispositivos móviles corporativos bajo su responsabilidad.
5. Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles.
6. No hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como Wifi, Bluetooth, en los dispositivos móviles.
7. No conectar los dispositivos móviles por puerto USB a cualquier computador público, de hoteles, internet, entre otros.
8. No almacenar videos, fotografías o información personal en los dispositivos móviles corporativos.

3. Política de uso de controles criptográficos y gestión de llaves.

- INTEGRA WEB, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la gestión segura de la información ha determinado realizar cifrado en los discos duros y utilizar plantilla de WordPress con certificado SSL para el sitio web.
- INTEGRA WEB, adaptándose al contexto actual de la pandemia del Covid 19 ha permitido trabajar desde computadores personales y por tanto, no se continua con el cifrado de discos duros.
- INTEGRA WEB, con el fin de asegurar las contraseñas de Wifi, serán cambiadas cada tres meses.
- Se realizarán revisiones de forma periódica (anualmente) en los controles criptográficos.

4. Política de teletrabajo

INTEGRA WEB, para la gestión integral en relación con su alcance respecto del teletrabajo, ha establecido lo siguiente considerando los requisitos aplicables conforme a lo declarado en la política general integral y bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

	Infraestructura/Sistemas		
ELEMENTO DEL ALCANCE	**Infr. - S.I propios**	**Infr. – S.I del cliente**	
a. Prestación servicios de gestión de la información y sistemas de información (Software como servicios)	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone
	No permitido	No permitido	HDD externo
b. Administración delegada de infraestructura tecnológica, de hardware y de software, propia y/o de terceros	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone

	No permitido	No permitido	HDD externo
c. Ingeniería de software	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone
	No permitido	No permitido	HDD externo

1. Integra Web Prohíbe el almacenamiento y procesamiento de los datos.
2. Solo se autoriza el teletrabajo desde equipos de cómputo asignados por la compañía o aquellos autorizados por seguridad de la información.
3. La conexión se debe realizar desde sitios seguros, preferiblemente desde redes domésticas.
4. Al retirar el equipo de la compañía debe velar por su cuidado no exponiéndolo, ni abandonándolo en lugares públicos o privados, y en viajes debe siempre tenerlo consigo llevándolo como equipaje de mano y nunca almacenándolo en la bodega de carga.
5. Todo uso indebido de la información y del entorno físico es responsabilidad del empleado.
6. Todo ordenador o dispositivo móvil correspondiente

5. Política de control de acceso

INTEGRA WEB, para la gestión integral en relación con su alcance respecto del teletrabajo, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- La asignación de derechos de acceso operará exclusivamente sobre una base contractual, de forma que será requisito la existencia de una relación contractual vigente entre las partes que determine específicamente que tipo de información va a estar en el dominio de quien suscribe el acuerdo, que acciones realizará sobre esa información y las razones de la misma.
- El ajuste y remoción de derechos de acceso será realizado inmediatamente finalice la relación contractual, y si es necesaria una etapa de transferencia, tales derechos de acceso estarán a cargo de quien recibe la información.
- Trimestralmente se realizarán actividades de revisión de derechos de acceso. De ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.
- Ante cambios en contexto (requisitos y contratos) se realizarán actividades de revisión de derechos de acceso. De ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.
- En el caso de medios externos y considerando su movilidad, el acceso incluirá responsabilidades sobre la posible pérdida y robo del medio externo.
- En el caso de archivo físico, especialmente de clientes, el acceso será dado en las instalaciones donde resida dicho archivo, sea en las instalaciones del cliente o en la organización (INTEGRA WEB) y no estará permitida la extracción parcial o total.
- Todo escenario de teletrabajo deberá ser explícitamente autorizado.
- La organización utilizará sistemas Wifi con no transmisión de su ID y solo se dará acceso a equipos de cómputo autorizados

6. Política de escritorio limpio y de pantalla limpia.

INTEGRA WEB, para la para la gestión integral en relación con su alcance respecto a cómo las personas que realizan trabajos para la organización o en nombre de ella mantienen documentos y en general archivos en su espacio de trabajo y áreas relacionadas, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- En los equipos de cómputo, mantener únicamente el ícono de papelera de reciclaje, el de sistema (cuando éste sea el caso) y las aplicaciones que por funcionalidad o configuración determinada deban estar allí ubicados.
- En cuanto a archivos digitales y enlaces, si bien se pueden mantener (de forma temporal) algunos ejemplares en el escritorio, la carpeta de descargas y de documentos, éstos deben ser eliminados o archivados donde corresponde cuando finalice su procesamiento o sea necesario que la persona a cargo se retire de la estación de trabajo, así sea solo momentáneamente.
- Sobre los archivos físicos, solo se pueden mantener ejemplares en el escritorio mientras son procesados y deben ser archivados donde corresponde cuando finalice su procesamiento o sea necesario que la persona a cargo se retire de su sitio de trabajo, así sea solo momentáneamente.
- Para los archivos digitales y físicos, se deberán aplicar los principios archivísticos de procedencia y de orden original para asegurar una adecuada organización de los datos.

7. Política de copia de respaldo

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a cómo asegura la disponibilidad e integridad de la información ante la ocurrencia de un incidente disruptivo del tipo pérdida o alteración de la información, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- El período mínimo de copias de seguridad es semanal.
- Cada persona que realice trabajos para la organización o en su nombre, con equipo de cómputo a su cargo, deberá realizar todas las actividades en Google Drive y protocolos SSH para crear copia de seguridad de las actividades o tareas que realizan diariamente.
- Luego de cada copia de seguridad, se deben verificar los medios (soporte físico donde fue hecha la copia de seguridad) para asegurar su funcionamiento.
- Se pueden mezclar estrategias de copia incremental (agregando los archivos nuevos o mejorados) o total (copiando totalmente la información objetivo)
- Las copias de seguridad deben estar segmentadas, de forma que cada carpeta o elemento de organización contenga únicamente datos y documentos relacionados con una temática.
- El medio donde se realiza la copia de seguridad debe estar ubicado en sitio externo a la oficina de INTEGRA WEB y resguardado ante una eventual pérdida de confidencialidad.

8. Políticas para la transferencia de información

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a cómo asegura la transferencia de información, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Toda transferencia de información (interna o externa, desde o hacia la organización) debe estar identificada contemplando como mínimo conjunto de datos, remitente, destinatario, medio de

transferencia y justificación de la misma. Para el caso de transferencias sucesivas, este elemento solo será identificado una única vez a menos que cambie el conjunto de datos.
- No está permitida la transferencia de información reservada o de carácter nacional fuera del territorio colombiano, lo cual incluye herramientas de acceso compartido.
- Toda transferencia de información debe generar su respectivo registro para asegurar trazabilidad.
- Ninguno de los usuarios de la empresa debería trabajar sobre el usuario administrador en su computador.
- Los usuarios normales (que no son administrador) deberían tener políticas restrictivas (ej. instalar o terminar aplicaciones).

9. Política de desarrollo seguro

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a acciones de desarrollo de software, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:
- Todo desarrollo, mantenimiento, prueba, implementación o cambio de software debe incluir la definición o aplicación de requisitos de seguridad en el software.
- En el caso que el cliente no especifique requisitos de seguridad en el software, la organización deberá establecer un estándar mínimo de requisitos de seguridad y aplicarlos.
- Todo desarrollo de software realizado con terceros o personal interno de la organización deberá contar con un acuerdo de transferencia de derechos patrimoniales de autor hacia la organización.

10. Política de seguridad de la información para relaciones con proveedores

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a partes interesadas que le provean productos o servicios relacionados o con impacto en la información, sean éstos personas naturales o jurídicas, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:
- Todo acuerdo, contrato o similar, propuesta comercial, deberá incorporar requisitos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.
- Todo acuerdo, contrato o similar, deberá incorporar requisitos de control y auditabilidad, según el riesgo, para poder conocer la aplicación de los lineamientos en seguridad de la información.

11. Política de seguridad de la información en gestión de proyectos

INTEGRA WEB, para la gestión integral en relación con su alcance sobre proyectos de cualquier tipo, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:
- Todo proyecto deberá incorporar requisitos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.

- Los proyectos que la organización determine como de riesgo medio o alto, deberán incluir su propia identificación y análisis de riesgos, así como sus controles respectivos.
- Todo proyecto deberá incorporar mecanismos de seguimiento, medición y control para poder conocer la aplicación de los lineamientos generales y específicos en seguridad de la información.
- Todo equipo de cómputo, de propiedad de la organización o alquilado, será utilizado de forma exclusiva para los fines de la organización en horarios laborales (lunes a viernes de 8:00 am a 12:00 m y de 2:00 pm a 6:00 pm y sábados de 9:00 am a 1: pm), solo permitiendo elementos públicos de transmisión de música (YouTube) con auriculares y en horarios de descanso (lunes a viernes de 12:00 m a 2:00 pm y de 6:00 pm a 8:00 pm, los sábados de 1:00 pm a 2:00 pm) es permitido jugar videojuegos Open Sours y utilizar aplicaciones para entretenimiento desde el navegador.

12. Política de instalación de software

INTEGRA WEB, para la gestión integral en relación con su alcance sobre instalación de software, incluyendo actualizaciones, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Toda instalación de software, incluidas actualizaciones, será realizada de forma manual por personal explícitamente autorizado por la organización.
- Antes de realizar cualquier instalación, se deberán realizar pruebas para determinar el nivel de riesgo asociado a ese software a ser instalado.
- Todo equipo de cómputo, de propiedad de la organización o alquilado, deberá tener deshabilitada la opción de instalación de software.

13. Política de gestión de licencias

- Los equipos que no se han propiedad de integra web y se les permita tener información de la organización es responsabilidad del funcionario o contratista contar con el software de su dispositivo debidamente licenciado.

14. Política de equipos desatendidos

INTEGRA WEB, para la gestión integral en relación con su alcance en los equipos desatendidos, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- - Los equipos de cómputo y móviles deben tener contraseña y se debe activar su protección a los dos minutos de inactividad.

15. Política de protección de datos

INTEGRA WEB, para la gestión integral en relación con su alcance en los datos de carácter personal, serán sometidos a los fines establecidos conforme a la ley 1581 de 2012 y sus decretos reglamentarios, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Cuando los datos sobre los cuales se esté brindando acceso sean de carácter personal, se deberá adicionalmente suscribir un acuerdo de transferencia y responsabilidad de datos personales.
- Sin importar los posibles derechos de acceso aplicables, está prohibida la copia, parcial o total, de datos, documentos y demás relacionados.
- Toda información manejada por la organización será para uso exclusivo de la misma.
- La utilización, copia, impresión, retención, divulgación, reenvío o cualquier acción no autorizada a la información de carácter personal será sancionada legalmente.

FIRMA DE APROBACIÓN

CAMILO ANDRÉS ECHEVERRY

Representante legal