

**Política de Integridad de OGUN, Soluciones en TI, S.A. de C.V.
(En cumplimiento del artículo 25 de la Ley General de Responsabilidades
Administrativas).**

Contents

I.	Manual de la Organización y Procedimientos.....	3
II.	Código de Ética y Conducta	16
III.	Sistemas Adecuados y Eficaces de Control, Vigilancia y Auditoría.....	20
IV.	Sistemas Adecuados De Denuncia.	23
V.	Sistemas y Procesos Adecuados de Entrenamiento y Capacitación.	24
VI.	Políticas de Recursos Humanos Tendientes a Evitar la Incorporación de Personas que Puedan Poner en Riesgo a la Integridad de la Corporación.....	27
VII.	Mecanismos que Aseguren en Todo Momento la Transparencia y Publicidad de sus Intereses.	31
	Anexos.	33
	Anexo A. Formatos y Documentos.....	33
	A.1 Formato de Declaración de Conflicto de Interés.	33
	A.2 Formato de Registro de Regalos.....	34
	A.3 Formato de Denuncia.	35
	Anexo B. Matriz de Riesgos de Integridad.	36
	B.1 Identificación de Riesgos por Proceso.	36
	B.2 Plan de Mitigación de Riesgos.	36
	Anexo C. Directorio de Contactos.	37
	C.1 Contactos Internos.....	37
	C.2 Canales de Denuncia.....	38
	C.3 Contactos Externos de Emergencia.	39

I. Manual de la Organización y Procedimientos.

OGUN Soluciones en TI S.A. de C.V.

Misión. Proteger los activos y optimizar las operaciones de nuestros clientes a través de tecnología avanzada, metodologías probadas y un equipo altamente capacitado, generando valor agregado que impulse el crecimiento y la competitividad de las organizaciones que confían en nosotros.

Visión. Ser la empresa líder en México y reconocida a nivel latinoamericano en la provisión de soluciones integrales de seguridad y tecnología empresarial, distinguiéndonos por su: innovación y excelencia.

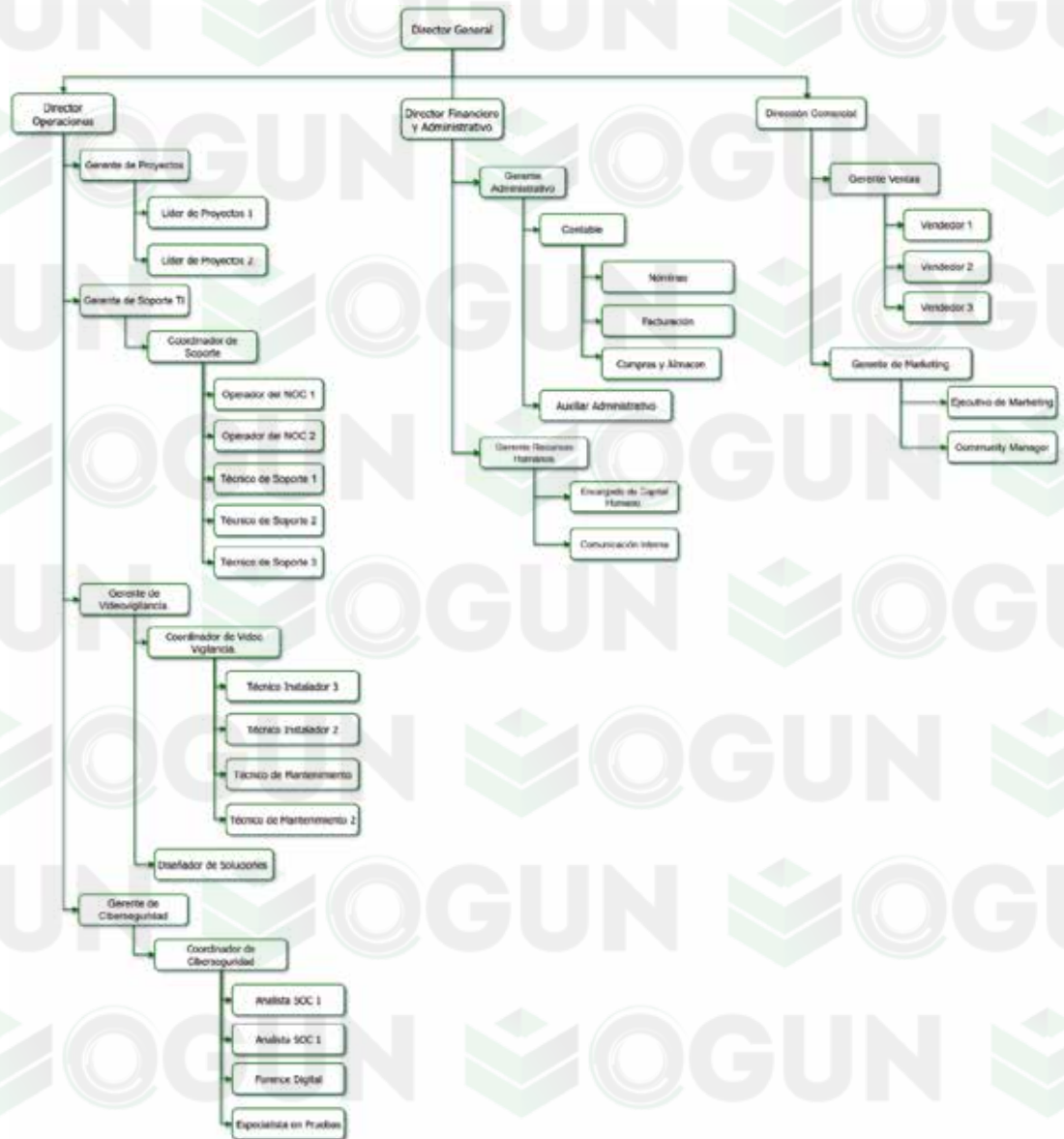
¿Qué hace la Empresa?

OGUN, Soluciones en TI, S.A. de C.V. se dedica, desde hace más de una década, a ofrecer servicios de Videovigilancia, Ciberseguridad, Infraestructura en TI y Consultoría.

Valores.

- **Integridad:** Actuar con honestidad y rectitud
- **Transparencia:** Apertura en la información y procesos
- **Legalidad:** Cumplimiento estricto del marco legal
- **Responsabilidad:** Rendición de cuentas por actos y decisiones
- **Eficiencia:** Optimización de recursos y procesos

Organigrama.



Función de Cada Puesto.

Director General. Responsable de la estrategia general de la empresa, la toma de decisiones clave y la supervisión de todas las áreas.

Director Operativo. Coordina y supervisa la ejecución técnica de los servicios y proyectos, asegurando la eficiencia operativa.

Gerente de Proyectos. Responsable de planificar, ejecutar y supervisar proyectos desde su inicio hasta su finalización. Sus funciones principales incluyen: Definir objetivos, alcance y entregables del proyecto, coordinar equipos multidisciplinarios, gestionar presupuestos y controlar costos, identificar y mitigar riesgos.

Líder de Proyecto. Planifica, ejecuta y da seguimiento a proyectos tecnológicos, asegurando cumplimiento de tiempos, costos y calidad.

Gerente de Videovigilancia. Supervisa y dirige todas las operaciones relacionadas con sistemas de videovigilancia en la organización.

Coordinador de videovigilancia: Supervisa instalaciones y mantenimiento de sistemas de videovigilancia.

Técnico Mantenimiento. Se encarga del mantenimiento preventivo y correctivo de cámaras, grabadores y equipos de vigilancia. Realiza diagnósticos, reparaciones, actualizaciones de firmware y garantiza el funcionamiento óptimo del sistema.

Técnico Instalador. Instala y configura sistemas completos de videovigilancia: cámaras, cableado, grabadores y software. Realiza pruebas de funcionamiento, capacita a usuarios y documenta las instalaciones realizadas.

Diseñador de Soluciones: Diseña arquitecturas técnicas para proyectos de seguridad y videovigilancia.

Gerente de Ciberseguridad. Lidera la estrategia de seguridad informática de la organización. Define políticas de seguridad, gestiona el presupuesto, supervisa equipos especializados y responde ante incidentes críticos de seguridad.

Coordinador de Ciberseguridad. Coordina la implementación de medidas de seguridad, monitorea amenazas, gestiona incidentes de seguridad y asegura el cumplimiento de políticas. Actúa como enlace entre el equipo técnico y la gerencia.

Analista SOC: Identifica y responde a incidentes de seguridad informática.

Especialista en Pruebas de Penetración: Realiza auditorías para detectar vulnerabilidades en sistemas.

Forense Digital / Respuesta a Incidentes: Investiga y documenta incidentes de seguridad.

Gerente de Soporte TI. Dirige el departamento de soporte técnico, establece procesos y estándares de servicio, gestiona recursos humanos

y tecnológicos, y asegura la satisfacción del usuario final en servicios de TI.

Coordinador de Soporte. Supervisa las actividades diarias del equipo de soporte, asigna tickets, monitorea métricas de rendimiento y coordina la resolución de incidentes complejos que requieren escalamiento.

Operador de NOC. Monitorea 24/7 la infraestructura de red desde el Centro de Operaciones de Red. Detecta incidentes, realiza diagnósticos iniciales, ejecuta procedimientos de respuesta y escala problemas cuando es necesario.

Técnico de Soporte. Proporciona asistencia técnica directa a usuarios finales, resuelve problemas de hardware y software, instala aplicaciones, realiza mantenimiento básico y documenta soluciones aplicadas.

Director Financiero y Administrativo. Responsable de supervisar todas las operaciones financieras y administrativas de la organización. Forma parte del equipo directivo y reporta directamente al CEO.

Gerente de Administrativo. Dirige y coordina todas las actividades administrativas y financieras de la empresa, asegurando el cumplimiento de las obligaciones fiscales, la eficiencia operativa y el soporte administrativo necesario para el crecimiento del negocio tecnológico.

Contable. Registra transacciones financieras, prepara estados financieros, realiza conciliaciones bancarias y asegura el cumplimiento de

obligaciones fiscales. Mantiene la contabilidad general de la empresa actualizada y precisa.

Nóminas. Calcula y procesa el pago de salarios, prestaciones y deducciones de empleados. Gestiona altas/bajas, vacaciones, incapacidades y cumple con obligaciones laborales y fiscales relacionadas con la nómina.

Facturación. Elabora y emite facturas a clientes, controla cuentas por cobrar, gestiona cobranzas y mantiene actualizados los registros de ventas. Asegura el cumplimiento de requisitos fiscales en la facturación.

Compras y Almacén. Gestiona adquisiciones de materiales y servicios, negocia con proveedores, controla inventarios y supervisa el almacenamiento. Optimiza costos y asegura disponibilidad de recursos para operaciones.

Auxiliar Administrativo. Brinda soporte administrativo general: archivo de documentos, atención telefónica, correspondencia, agenda de reuniones y tareas de apoyo a diferentes departamentos según necesidades.

Gerente de Recursos Humanos. El Gerente de Recursos Humanos diseña e implementa las estrategias necesarias para atraer, seleccionar y retener el talento especializado para desempeñar tareas en TI. Debe impulsar iniciativas de capacitación, desarrollo profesional y gestión del desempeño para asegurar que el equipo cuente con las habilidades

necesarias y oportunidades de crecimiento. Fomenta una cultura organizacional positiva, inclusiva y productiva. Supervisa la gestión de nóminas:

Encargado de Capital Humano. Gestiona procesos de reclutamiento, selección, capacitación y desarrollo del personal. Administra políticas de recursos humanos, evaluaciones de desempeño y clima laboral.

Comunicación Interna. Desarrolla y ejecuta estrategias de comunicación entre empleados, gestiona canales internos, organiza eventos corporativos y fortalece la cultura organizacional.

Director Comercial. Lidera la estrategia comercial de la empresa, define objetivos de ventas, supervisa equipos comerciales y de marketing, y toma decisiones estratégicas para incrementar ingresos y market share.

Gerente de Ventas. Supervisa el equipo de vendedores, establece metas de venta, desarrolla estrategias comerciales, gestiona cuentas clave y reporta resultados. Coordina actividades para alcanzar objetivos comerciales.

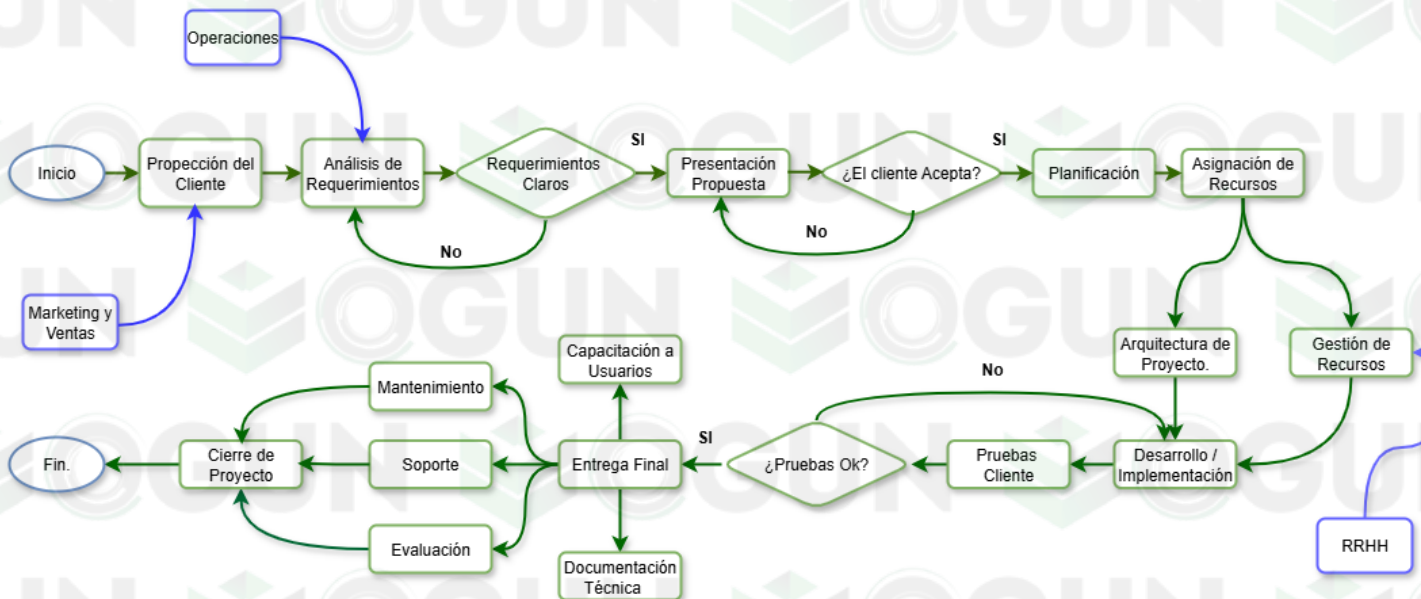
Vendedor. Prospectivo clientes, presenta productos/servicios, negocia condiciones de venta y cierra operaciones comerciales. Mantiene relaciones con clientes existentes y busca nuevas oportunidades de negocio.

Gerente de Marketing. Dirige estrategias de marketing, supervisa campañas publicitarias, analiza mercado y competencia, gestiona presupuestos de marketing y coordina equipos creativos y digitales.

Ejecutivo de Marketing. Ejecuta campañas de marketing, realiza investigación de mercado, coordina eventos promocionales, gestiona proveedores de publicidad y apoya en el desarrollo de materiales promocionales.

Community Manager. Gestiona presencia digital de la marca en redes sociales, crea contenido, interactúa con la comunidad online, monitorea reputación digital y ejecuta estrategias de marketing digital.

Proceso General de la Empresa.



Actividades de la Empresa.

Prospección de Clientes. El área de Ventas y Marketing realizan la prospección de clientes y es el proceso sistemático de identificar y contactar potenciales clientes que puedan necesitar servicios de TI. Incluye investigación de mercado para identificar empresas con necesidades tecnológicas, análisis de sectores específicos, generación de leads a través de marketing digital, networking en eventos del sector, y contacto directo con tomadores de decisiones.

Análisis de Requerimientos. El Análisis de Requerimientos es realizado por el área de Ventas y Operaciones. Esta actividad consiste en comprender profundamente las necesidades técnicas y de negocio del cliente. Involucra entrevistas con stakeholders clave, levantamiento de procesos actuales, identificación de problemas y oportunidades de mejora, definición de objetivos específicos del proyecto, y documentación detallada de requisitos funcionales y no funcionales. Se analizan restricciones técnicas, presupuestarias y de tiempo, y se valida la información con el cliente para asegurar una comprensión completa y precisa de sus expectativas.

Prospección de Clientes. El área de Ventas y Marketing realizan la prospección de clientes y es el proceso sistemático de identificar y contactar potenciales clientes que puedan necesitar servicios de TI. Incluye investigación de mercado para identificar empresas con necesidades tecnológicas, análisis de sectores

específicos, generación de leads a través de marketing digital, networking en eventos del sector, y contacto directo con tomadores de decisiones.

Análisis de Requerimientos. El Análisis de Requerimientos es realizado por el área de Ventas y Operaciones. Esta actividad consiste en comprender profundamente las necesidades técnicas y de negocio del cliente. Involucra entrevistas con stakeholders clave, levantamiento de procesos actuales, identificación de problemas y oportunidades de mejora, definición de objetivos específicos del proyecto, y documentación detallada de requisitos funcionales y no funcionales. Se analizan restricciones técnicas, presupuestarias y de tiempo, y se valida la información con el cliente para asegurar una comprensión completa y precisa de sus expectativas.

Presentación de Propuesta. Operaciones elabora propuestas técnicas y comerciales, combina los requerimientos identificados con las capacidades de la empresa. Incluye diseño de la solución técnica, definición del alcance del proyecto, estimación de tiempos y costos, identificación de entregables específicos, y estructuración de la propuesta de valor.

Planificación. La planificación de proyectos establece la hoja de ruta para la ejecución exitosa. Comprende la creación de planes detallados de trabajo, definición de fases, establecimiento de cronogramas, identificación de dependencias entre tareas, y análisis de riesgos potenciales. Se desarrollan estructuras de desglose del trabajo (WBS), se definen criterios de éxito para cada fase, se establecen procesos de comunicación y reporting, y se crean planes de contingencia para mitigar riesgos identificados.

Asignación de Recursos. Este proceso involucra la selección y asignación del personal más adecuado para cada proyecto. Incluye evaluación de habilidades técnicas requeridas, análisis de disponibilidad del equipo, balanceo de cargas de trabajo, y formación de equipos multidisciplinarios. Se consideran las fortalezas individuales, experiencia previa en proyectos similares, y se asegura que el equipo tenga las competencias necesarias para cumplir con los objetivos del proyecto dentro de los tiempos establecidos.

Gestión de Recursos. La gestión de recursos abarca la administración integral de todos los activos necesarios para el proyecto. Incluye gestión de recursos humanos (desarrollo de talento, evaluación de desempeño), gestión de recursos tecnológicos (hardware, software, licencias), administración de presupuestos, y optimización de la utilización de recursos. Se monitorea constantemente el rendimiento del equipo, se identifican necesidades de capacitación, y se asegura que los recursos estén disponibles cuando se necesiten.

Arquitectura de Proyectos. La arquitectura de proyectos define la estructura técnica y organizacional de la solución. Comprende el diseño de la arquitectura en la nube, definición de tecnologías a utilizar, estructuración de componentes del sistema, establecimiento de patrones de diseño, y creación de documentación técnica.

Implementación. Fase de desarrollo donde se construye la solución tecnológica según las especificaciones y diseño previamente definidos. Se utilizan metodologías ágiles con sprints y revisiones continuas para asegurar el progreso adecuado.

Pruebas con el Cliente. Validación del sistema en un ambiente controlado con la participación directa del cliente. Se realizan pruebas de aceptación de usuario (UAT) donde el cliente verifica que la solución cumple con sus expectativas y requerimientos de negocio. Se documenta el feedback y se priorizan los ajustes necesarios antes de la entrega final.

Entrega Final. Despliegue del sistema completo en el ambiente de producción del cliente. Incluye la migración de datos, configuración de servidores, instalación de software y puesta en marcha del sistema. Se verifica que todo funcione correctamente en el ambiente real y se proporciona acceso a los usuarios finales con sus respectivos permisos y configuraciones.

Capacitación a Usuarios. Transferencia de conocimiento para que los usuarios finales puedan operar el sistema eficientemente. Se crean materiales didácticos, se realizan sesiones prácticas y se resuelven dudas. El objetivo es asegurar la adopción exitosa del sistema por parte de la organización.

Documentación Técnica. Creación de manuales y guías que describen la arquitectura, funcionalidades, procedimientos de operación y mantenimiento del sistema. Incluye documentación para usuarios finales, administradores del sistema y desarrolladores. Se elaboran diagramas técnicos, especificaciones de APIs, guías de instalación y procedimientos de respaldo y recuperación.

Soporte. Servicio continuo de asistencia técnica post-implementación para resolver incidencias, dudas operativas y problemas técnicos. Se establece un

canal de comunicación directo con el cliente, se categorizan las consultas por prioridad y se proporciona respuesta dentro de los tiempos acordados. Incluye soporte remoto, telefónico y en sitio según sea necesario.

Mantenimiento. Actividades programadas para asegurar el funcionamiento óptimo del sistema a largo plazo. Incluye actualizaciones de software, parches de seguridad, optimización de bases de datos, monitoreo de rendimiento y mantenimiento preventivo. Se planifican ventanas de mantenimiento para minimizar el impacto en las operaciones del cliente.

Evaluación del Proyecto. Análisis integral del proyecto completado para identificar lecciones aprendidas, medir el cumplimiento de objetivos y evaluar la satisfacción del cliente. Se revisan métricas de tiempo, costo, calidad y alcance. Se documenta el desempeño del equipo, se identifican mejores prácticas y áreas de oportunidad para proyectos futuros.

Cierre del Proyecto. Proceso formal de finalización que incluye la entrega de todos los entregables, firma de actas de aceptación, liberación de recursos del proyecto y archivo de documentación. Se realiza una reunión de cierre con el cliente, se transfieren las responsabilidades al equipo de soporte y mantenimiento, y se documenta oficialmente la conclusión exitosa del proyecto.

II. Código de Ética y Conducta.

OGUN, soluciones en TI, S.A. de C.V., establece que ningún integrante de su plantilla laboral debe efectuar en forma alguna, cualquier tipo de fraude, soborno o actos de corrupción dentro de sus actividades. Por tal motivo sus colaboradores no deberán solicitar, aceptar, ofrecer o dar ningún tipo de soborno en el ejercicio de sus responsabilidades, a nombre propio ni de la empresa.

OGUN, Soluciones en TI, S.A. de C.V., evita tener relaciones con empresas y entidades que son conocidas o se tienen indicios de que realicen y acepten sobornos y actos de corrupción. Nuestros colaboradores no podrán sufrir ninguna represalia, sanción o consecuencia por negarse a ser partícipe de entregar o recibir algún soborno, aun cuando esto represente la pérdida de una negociación o trato.

Valores.

Los Valores de OGUN, Soluciones en TI, son:

Integridad

- Actuar con honestidad en todas las actividades
- Ser congruente entre valores y acciones
- Mantener consistencia en el comportamiento

Respeto

- Tratar a todas las personas con dignidad
- Valorar la diversidad y la inclusión
- Escuchar y considerar diferentes perspectivas

Responsabilidad

- Cumplir compromisos adquiridos
- Asumir consecuencias de decisiones
- Rendir cuentas por resultados

Transparencia

- Proporcionar información clara y veraz
- Facilitar el acceso a información pública
- Comunicar decisiones de manera abierta

Prohibiciones.

- **Corrupción:** Ofrecer, solicitar o recibir sobornos
- **Conflicto de interés:** Anteponer intereses personales
- **Abuso de poder:** Usar posición para beneficio personal
- **Discriminación:** Tratos desiguales por características personales
- **Acoso:** Comportamientos intimidatorios o hostiles

Obligaciones Específicas.

- **Confidencialidad:** Proteger información sensible
- **Uso adecuado de recursos:** Emplear bienes corporativos apropiadamente
- **Cumplimiento normativo:** Acatar leyes y reglamentos
- **Reporte de irregularidades:** Comunicar posibles faltas
- **Capacitación continua:** Participar en programas de formación

Relaciones con Terceros.

Proveedores.

- Selección objetiva y transparente
- Evitar regalos o beneficios indebidos
- Mantener relaciones profesionales
- Cumplir términos contractuales

Clientes.

- Proporcionar información veraz
- Proteger datos personales
- Ofrecer productos/servicios de calidad
- Atender quejas y reclamos

Autoridades.

- Cooperar en investigaciones
- Proporcionar información requerida
- Mantener relaciones institucionales apropiadas
- Cumplir obligaciones regulatorias

Consultar formatos de Conflicto de Intereses, Registro de Regalos en Anexo A.

Sanciones Por incumplimientos.

- **Amonestación verbal:** Para faltas menores
- **Amonestación escrita:** Para faltas leves
- **Suspensión:** Para faltas graves
- **Terminación de relación laboral:** Para faltas muy graves

Procedimiento disciplinario.

1. Notificación de la falta
2. Oportunidad de defensa
3. Investigación y análisis
4. Determinación de sanción
5. Aplicación de medida disciplinaria.

Difusión de Código de Conducta

La presente Política, así como nuestro Código de Ética y Conducta, deben de ser difundidas a través de los medios corporativos, incluido

nuestro sitio web <https://ogunsolucionesti.com> y el envío masivo de correo electrónico, con el objetivo de que puedan ser consultados por

todos nuestros colaboradores y el público en general.

Difusión Interna.

Correo electrónico institucional: El envío masivo de correo electrónico, a todos los empleados, con el código de ética y conducta de la organización, ha sido establecido como medio de difusión preferente. Se realizan comunicados oficiales, recordatorios periódicos y actualizaciones al código.

Cartelería y señalización: Se han realizado Carteles informativos, colocados en áreas comunes, oficinas, salas de reuniones y espacios de trabajo con los principios fundamentales de dicho código.

Difusión Externa.

Sitio web corporativo: OGUN pone a la disposición del público general y de sus colaboradores el sitio: <https://ogunsolucionesti.com/>, donde estarán publicados nuestro código de ética y la presente política de Integridad Empresarial, con fácil acceso desde el menú principal.

III. Sistemas Adecuados y Eficaces de Control, Vigilancia y Auditoría.

Para asegurar la observancia continua del Programa de Integridad y mitigar los riesgos identificados, OGUN, Soluciones en TI, ha implementado un marco de Control Interno, Vigilancia y Auditoría diseñado para detectar, prevenir y responder a cualquier acto contrario a nuestro Código de Conducta o a la normativa vigente. Con dicho marco se ha constituido un Comité de Vigilancia, el cual actúa como órgano colegiado responsable de supervisar, evaluar y dar seguimiento al cumplimiento de los principios éticos, normativas internas y disposiciones legales aplicables.

El Comité de Vigilancia está conformado por representantes de las siguientes áreas clave:

- Dirección General, quien preside el comité y asegura el respaldo institucional.
- Oficial de Cumplimiento, encargado de coordinar la implementación de la política y de canalizar los reportes.
- Recursos Humanos, responsable de incorporar criterios de integridad en los procesos laborales y disciplinarios.
- Auditoría Interna, quien proporciona elementos de control y verificación.
- Asesoría Jurídica, para la interpretación y aplicación conforme a la normativa vigente.

Las principales funciones del Comité son:

- Supervisar el cumplimiento de la Política de Integridad en todos los niveles de la organización.
- Atender y dar seguimiento a los reportes de posibles violaciones éticas o conductas inapropiadas.
- Emitir recomendaciones para prevenir, corregir o sancionar situaciones contrarias a la integridad institucional.
- Revisar periódicamente la vigencia, pertinencia y eficacia de la política, proponiendo ajustes cuando sea necesario.

- Promover la cultura ética, mediante acciones de sensibilización, capacitación y comunicación interna.

Los responsables del Comité de Vigilancia son:

Rol	Nombre	Puesto.
Director	Silvestre David	Director de Operaciones
Oficial de cumplimiento	Ricardo Cano Baltazar	Director General
Líder de RRHH.	Isaac Ulises Carrillo Alarcón	Gerente de Recursos Humanos
Líder Legal	Javier Cortés Rubio	Abogado
Líder Auditoría	Ricardo Gómez Lemus	Director Financiero

Sistema de Control Interno

El control interno es un proceso continuo e inherente a todas las actividades de la Corporación. Se basa en los siguientes pilares:

- **Separación de Funciones (Segregación de Deberes):**
 - Se implementarán controles para garantizar que ninguna persona, o un grupo reducido de personas, posea control total sobre un proceso de alto riesgo o una transacción financiera crítica, tales como la autorización, ejecución, registro y custodia.
- **Controles Financieros y Operacionales:**
 - Se establecerán límites de autorización escalonados para gastos, adquisiciones y compromisos contractuales, requiriendo la aprobación de múltiples niveles gerenciales o directivos según el monto.
 - Se exigirá la doble firma para la liberación de pagos significativos y se realizarán conciliaciones bancarias y de cuentas de forma periódica e independiente.
 - Todos los desembolsos deben contar con documentación soporte completa y verificable que acredite el propósito, la necesidad y la razonabilidad del gasto.
- **Políticas y Procedimientos Documentados:**
 - Todos los procesos críticos (compras, ventas, contratación, pagos a terceros) deben estar documentados y formalizados,

sirviendo como base para cualquier revisión o auditoría posterior.

Vigilancia y Monitoreo Continuo

La vigilancia es una función proactiva cuyo objetivo es identificar patrones de comportamiento o transacciones inusuales que puedan indicar un riesgo de integridad.

- **Monitoreo de Transacciones de Alto Riesgo:**
 - Se implementan herramientas de análisis de datos para monitorear transacciones recurrentes con partes relacionadas, pagos a consultores o intermediarios en jurisdicciones de alto riesgo, y cualquier gasto que no se ajuste a la naturaleza del negocio.
- **Supervisión Jerárquica:**
 - Los superiores son responsables de la vigilancia activa de las actividades de su equipo y deben reportar inmediatamente cualquier incumplimiento o conducta sospechosa al área de Cumplimiento.
- **Evaluación Periódica de Riesgos:**
 - El área de Cumplimiento o Auditoría Interna realiza una revisión anual formal de los riesgos de corrupción, fraude y ética, ajustando los controles internos en función de los nuevos riesgos detectados. Ver Anexo B.

Función de Auditoría Interna

La Auditoría Interna es una función independiente y objetiva de aseguramiento y consulta, diseñada para agregar valor y mejorar las operaciones de la Corporación.

- **Auditorías Basadas en el Riesgo:**
 - Los planes de Auditoría Interna se fundamentarán en la Matriz de Riesgos de Integridad de la Corporación, focalizando los esfuerzos de revisión en los

procesos y áreas de mayor vulnerabilidad (ej. Cumplimiento contractual, procesos de licitación, gestión de activos).

- **Acceso Total a la Información:**

- El equipo de Auditoría Interna tendrá total y libre acceso a toda la información, registros, sistemas, colaboradores e instalaciones que sean necesarios para el cabal cumplimiento de su función de verificación.
- Su función reporta directamente al Comité de Auditoría del Consejo (o al máximo órgano de gobierno) para preservar su independencia de la administración ejecutiva.

- **Reporte Directo:**

- Los resultados de las auditorías de cumplimiento o integridad son reportados directamente al Comité de Auditoría o al Comité de Ética (o al más alto órgano de gobierno), asegurando la independencia y la acción oportuna de la alta dirección.

Estos sistemas garantizan que la integridad no es solo una declaración de principios, sino una realidad operativa que se verifica y se protege constantemente.

IV. Sistemas Adecuados De Denuncia.

Canales Disponibles (24/7)

Canal	Contacto	Confidencialidad	Tiempo de Respuesta.
Email	integridad@ogun.com.mx	Alta	24 horas
WhatsApp	56 1260 9340	Alta	2 horas en horario laboral

Proceso de Investigación

- **Recepción y folio** (Día 1). Ver Formato en Anexo A.
- **Evaluación preliminar** (Días 2-5)
- **Investigación detallada** (Días 6-20)
- **Dictamen y medidas** (Días 21-28)
- **Comunicación de resultado** (Días 29-30)

PROTECCIÓN AL DENUNCIANTE:

- Confidencialidad absoluta
- Prohibición de represalias (sancionable con despido)
- Seguimiento del caso hasta su conclusión
- Derecho a asesoría legal externa si es necesario

V. Sistemas y Procesos Adecuados de Entrenamiento y Capacitación.

OGUN, Soluciones en TI, se compromete a mantener un alto estándar de integridad y ética en todas sus operaciones. Para garantizar que cada miembro del equipo comprenda y aplique nuestra Política de Integridad, hemos establecido un sistema de entrenamiento y capacitación.

El objetivo principal es asegurar que todo el personal, desde la alta dirección hasta los nuevos ingresos, esté plenamente consciente de las leyes, regulaciones, códigos de conducta y políticas internas relevantes para su rol. Además, se busca fomentar las habilidades necesarias para identificar y manejar dilemas éticos y situaciones de riesgo, y promover una cultura de cumplimiento donde la integridad sea un valor central e innegociable.

Nuestro sistema de entrenamiento y capacitación incluye, pero no se limita a, los siguientes componentes:

- **Programa de Inducción Obligatoria:** Todo nuevo colaborador debe completar un curso exhaustivo sobre la **Política de Integridad** de la empresa, el **Código de Conducta** y los procedimientos de denuncia al inicio de su relación laboral.
- **Entrenamiento Especializado por Función:** Se ofrecerá capacitación más profunda y detallada a los empleados en roles de alto riesgo (ej. Ventas, Adquisiciones, Finanzas), enfocada en los riesgos de integridad inherentes a sus responsabilidades.

Programa de Inducción Obligatoria.

PROGRAMA DE 4 HORAS:

1. Política de Integridad y Código de Conducta
2. Casos prácticos del sector T
3. Sistema de denuncias y protección
4. Evaluación y firma de compromiso

EVALUACIÓN MÍNIMA APROBATORIA: 85%.

Capacitación Especializado por Puesto

Personal Directivo.

Curso: Marco legal anticorrupción (4 horas)

- 1.1. Fundamentos y Consecuencias de la Corrupción
- 1.2. Nuestro Marco Legal Clave
- 1.3. La Defensa de la Empresa
- 2.1. Conflictos de Interés: Detección y Declaración
- 2.2. Regalos, Viajes y Cortesías
- 2.3. Terceros y Due Diligence
- 3.1. Integridad Contable
- 3.2. Controles Clave
- 4.1. El Canal de Denuncia (Línea Ética)

4.2. Evaluación Final y Cierre

EVALUACIÓN MÍNIMA APROBATORIA: 85%.

Área Comercial

Curso: Ética en ventas y contratación pública (4 horas)

- 1.1. El Rol de Ventas como Alto Riesgo de Integridad
- 1.2. Regalos, Viajes y Cortesías: La Línea Roja
- 1.3. Conflictos de Interés en el Cliente Privado
- 2.1. El Proceso de Licitación con Integridad
- 2.2. Interacción con Funcionarios Públicos
- 2.3. Transparencia en la Facturación y Documentación
- 3.1. Riesgo en Agentes e Intermediarios Comerciales
- 3.2. Ética en las Compras (Proveedor-Contratista)
- 3.3. Integridad Contable en el Ciclo de Ventas
- 4.1. Canal de Reporte y Protección
- 4.2. Evaluación y Cierre

EVALUACIÓN MÍNIMA APROBATORIA: 85%.

Personal Técnico

Integridad en la ejecución de proyectos (4 horas)

- 1.1. Puntos de Riesgo en la Ejecución de Proyectos
- 1.2. Fraude en Proyectos
- 1.3. Integridad en el Liderazgo del Proyecto
- 2.1. Selección y Contratación Ética de Terceros
- 2.2. Conflicto de Interés con Subcontratistas
- 2.3. Control de Calidad y Fraude en Materiales
- 3.1. Gestión Transparente de Órdenes de Cambio (Change Orders)

3.2. Certificación de Avance de Obra (Estimaciones)

3.3. Integridad Contable en la Liquidación

Personal Administrativo

Curso: Controles internos y prevención de fraudes (4 horas)

1.1. ¿Qué es el Control Interno y por qué nos importa?

1.2. El Triángulo del Fraude y sus Consecuencias

1.3. Riesgos Clave en OGUN, Soluciones Tecnológicas.

2.1. Separación de Funciones (Segregación de Deberes)

2.2. Controles de Acceso y Autorización

2.3. Integridad y Documentación de Registros

3.1. Monitoreo y Conciliaciones

3.2. Controles Físicos y de Inventario

3.3. El Rol de la Auditoría Interna

4.1. El Deber de Reportar Fallas de Control

4.2. Evaluación y Compromiso

EVALUACIÓN MÍNIMA APROBATORIA: 85%.

VI. Políticas de Recursos Humanos Tendientes a Evitar la Incorporación de Personas que Puedan Poner en Riesgo a la Integridad de la Corporación.

Objetivo: Garantizar, a través de rigurosos procesos de Recursos Humanos, la incorporación exclusiva de personal idóneo y probo que se comprometa plenamente con el Código de Conducta y la ética

corporativa, mitigando de manera proactiva cualquier riesgo de corrupción o fraude desde el origen de la relación laboral.

La Política de Integridad de OGUN, Soluciones en TI, se refuerza desde el proceso de selección y contratación, reconociendo que la prevención es la herramienta más eficaz para salvaguardar el capital reputacional, ético y financiero de la Corporación. Por ello, se establecen las siguientes directrices y filtros obligatorios en todos los procesos de Recursos Humanos (RR.HH.):

1. Proceso de Selección Riguroso y Verificación de Antecedentes

Todo candidato a ocupar un puesto en OGUN, Soluciones en TI, será sometido a un proceso de selección que incluye, de forma enunciativa y no limitativa, las siguientes fases de verificación:

- Verificación de Referencias Laborales: Se realizarán consultas obligatorias a los empleadores previos para confirmar la trayectoria y el desempeño laboral, haciendo especial énfasis en la conducta ética y la observancia de normativas internas.
- Comprobación de Antecedentes: En cumplimiento con la legislación aplicable, RR.HH. podrá realizar la verificación de antecedentes penales, crediticios y laborales relevantes que puedan indicar un riesgo potencial para la Corporación (como fraudes, incumplimientos fiduciarios, o faltas graves de probidad).
- Validación de Credenciales: Se verificará la autenticidad de todos los títulos académicos, certificaciones profesionales y experiencia laboral declarada por el candidato.

2. Evaluación de Idoneidad Ética y Transparencia

Más allá de las competencias técnicas, el proceso de reclutamiento evaluará la idoneidad ética del aspirante para el puesto.

- Entrevistas Basadas en Competencias de Integridad: Se incluirán preguntas de carácter situacional y conductual diseñadas para evaluar la comprensión y el compromiso del candidato con los valores y el Código de Conducta de OGUN, Soluciones en TI.
- Declaración de Ausencia de Conflicto de Intereses: El candidato deberá firmar una declaración formal en la que manifieste la inexistencia de cualquier relación o situación que configure un conflicto de interés actual o potencial con la Corporación. Esta declaración será un requisito indispensable para la formalización del contrato.

3. Compromiso Inicial con la Integridad Corporativa

Previo a la incorporación y a la firma del contrato laboral:

- Reconocimiento y Aceptación del Código: Todo nuevo colaborador deberá recibir, leer y firmar un acuse de recibo y aceptación del Código de Conducta y la Política de Integridad de la Empresa, comprometiéndose expresamente a su cumplimiento irrestricto.
- Inducción Obligatoria en Integridad: La capacitación inicial de todo nuevo colaborador incluirá, de manera prioritaria y obligatoria, un módulo de inducción exhaustivo sobre Ética, Anticorrupción y Prevención de Delitos, con especial énfasis en el canal de denuncias y las consecuencias del incumplimiento.

Estas políticas aseguran que el personal que se incorpora a OGUN, Soluciones en TI, comparte y se compromete activamente con los más altos estándares de honestidad y probidad, minimizando así el riesgo de afectaciones a la integridad y reputación de la empresa.

Política de No discriminación:

En OGUN, Soluciones en TI, nos comprometemos a generar un ambiente de trabajo libre de discriminación, acoso y represalias. Valoramos la diversidad y promovemos la igualdad de oportunidades para todas las personas, independientemente de sus características personales.

La presente política aplica a:

- Todos los empleados, directivos y personal de la organización
- Procesos de reclutamiento, selección y contratación
- Desarrollo profesional, promociones y compensaciones
- Proveedores, contratistas y socios comerciales
- Clientes y beneficiarios de nuestros servicios

En OGUN queda prohibida cualquier forma de discriminación basada en:

- Raza, color y origen étnico
- Género, identidad de género y expresión de género
- Orientación sexual
- Edad

- Religión o creencias
- Discapacidad física o mental
- Estado civil o familiar
- Embarazo o maternidad/paternidad
- Nacionalidad o estatus migratorio
- Opiniones políticas
- Condición socioeconómica
- Apariencia física
- Cualquier otra característica protegida por ley

Se prohíben expresamente:

- Discriminación directa o indirecta en cualquier decisión laboral
- Acoso verbal, físico, psicológico o sexual
- Comentarios, bromas o gestos ofensivos o despectivos
- Exclusión deliberada de actividades laborales o sociales
- Represalias contra quien denuncie actos discriminatorios
- Creación de ambientes hostiles o intimidatorios

Las personas que experimenten o presencien discriminación pueden:

- Reportar el incidente al departamento de Recursos Humanos
- Utilizar el canal de denuncias confidencial: Buzón de Quejas
- Contactar al Comité de Ética e Integridad

¿Cómo evitar que el nuevo personal que ingrese no incumpla con las normas internas y la política de integridad?

Para evitar que el nuevo personal incumpla con las normas internas y la política de integridad, es fundamental implementar un proceso integral que comience desde la selección, realizando verificaciones exhaustivas de antecedentes y referencias, así como evaluaciones de valores éticos durante las entrevistas. Una vez contratado, el personal debe participar en un programa estructurado que incluya inducción obligatoria sobre cultura organizacional, entrega y firma del código de ética, capacitación

en políticas clave de integridad, y asignación de un mentor que modele comportamientos éticos durante los primeros meses. Es esencial mantener comunicación clara mediante manuales accesibles, capacitaciones continuas (anuales y específicas por rol), y canales de consulta disponibles donde puedan resolver dudas sobre dilemas éticos sin temor a represalias.

El monitoreo durante el periodo de prueba debe incluir evaluaciones específicas de cumplimiento normativo a los 30, 60 y 90 días, mientras que el liderazgo debe ejemplificar la integridad aplicando consecuencias consistentes ante violaciones, sin excepciones, y reconociendo públicamente las conductas íntegras. Finalmente, se deben establecer canales confidenciales de denuncia operados idealmente por terceros, declaraciones periódicas de conflicto de intereses, y un sistema de indicadores (KPIs) que permita medir la efectividad del programa y ajustarlo continuamente, creando así una cultura donde la integridad sea percibida no como una opción, sino como el fundamento innegociable de la organización.

VII. Mecanismos que Aseguren en Todo Momento la Transparencia y Publicidad de sus Intereses.

El compromiso de OGUN, Soluciones en TI, con la transparencia, la integridad y la comunicación efectiva requiere el uso sistemático de canales que aseguren que la información crítica, las políticas y los valores lleguen a todos los grupos de interés de manera oportuna, clara y verificable.

Los principales Medios de Difusión empleados por la Corporación son:

Página web: ogunsolucionesti.com

Instagram: www.instagram.com/ogunsoluciones.ti/

X: x.com/ogunsoluciones

LinkedIn: www.linkedin.com/company/ogun-soluciones-en-ti/

OGUN, Soluciones en TI, asegura que todos los documentos y comunicados emitidos a través de estos canales cumplen con los

principios de veracidad, objetividad y oportunidad. La utilización y consulta periódica de estos medios es una responsabilidad inherente a todos los miembros de la Empresa y sus grupos de interés.

Anexos.

Anexo A. Formatos y Documentos.

A.1 Formato de Declaración de Conflicto de Interés.

Declaración de Conflicto de Intereses.					
Nombre del empleado.			Fecha	dd/mm/aaaa	
Puesto.		Departamento.			
Situación Reportada:					
Partes involucradas					
Tipo de Interés.	<input type="checkbox"/> Económico	<input type="checkbox"/> Familiar	<input type="checkbox"/> Personal.	<input type="checkbox"/> Profesional.	<input type="checkbox"/> Otro
Medidas Propuestas.					
Número de Caso.		Fecha Recepción			
Firma del Empleado					

A.3 Formato de Denuncia.

FORMATO DE DENUNCIA INTERNA			
INFORMACIÓN DEL DENUNCIANTE (Opcional - puede ser anónima):			
Nombre:		Teléfono	
E-Mail		Área	
INFORMACIÓN DE LA DENUNCIA:			
Fecha del incidente		Lugar del incidente	
Personas involucradas.			
Descripción de los hechos.			
Evidencias disponibles.			
<input type="checkbox"/> Documentos:	<input type="checkbox"/> Fotografías:	<input type="checkbox"/> Video:	<input type="checkbox"/> Testigos: <input type="checkbox"/> Otros:
¿Desea mantener la denuncia anónima?		<input type="checkbox"/> Sí.	<input type="checkbox"/> No.
¿Autoriza ser contactado para aclaraciones?		<input type="checkbox"/> Sí.	<input type="checkbox"/> No.
Fecha de presentación.			

Anexo B. Matriz de Riesgos de Integridad.

B.1 Identificación de Riesgos por Proceso.

Proceso	Riesgo Identifica	Probabilidad	Impacto	Niveles de Riesgo	Controles	Controles Adicionales
Contrataciones	Favoritismo	Media	Alto	Alto	Comité de Selección	Evaluación Ciega
Compras	Soborno a Proveedor	Baja	Alto	Medio	Cotizaciones Múltiples	Rotación de Compradores
Ventas	Precios preferenciales	Media	Medio	Medio	Lista de Precios	Aprobación Gerencial
Finanzas	Malversación de Fondos	Baja	Muy Alto	Alto	Segregación de Funciones	Auditoria Continua.
Recursos Humanos	Nepotismo	Media	Medio	Medio	Políticas de Contratación	Verificación de Referencias.

B.2 Plan de Mitigación de Riesgos.

Para cada riesgo identificado:

- Descripción del riesgo
- Impacto potencial
- Controles preventivos
- Controles detectivos
- Plan de respuesta
- Responsable de monitoreo
- Frecuencia de revisión

Anexo C. Directorio de Contactos.

C.1 Contactos Internos.

OFICIAL DE CUMPLIMIENTO

Nombre: Ricardo Cano Baltazar

Teléfono: 56 1260 9340 Ext. 03

Correo: servicios@ogunsolucionesti.com

Ubicación: Dirección General, Prolongación Paseo de la Reforma 51 Oficina 604 Piso 6. Col. Paseo de las Lomas, C. P. 01330, Álvaro Obregón, CDMX

COMITÉ DE ÉTICA, HONOR E INTEGRIDAD

Presidente: Ricardo Cano Baltazar.

Secretario: Javier Cortés Rubio. Director Jurídico.

Vocales: Daniel Vallejo Salazar (Operaciones), Nayeli Sánchez Ruiz, (Ventas), Valeria Ximena Nava Rojas (Administración.)

AUDITORÍA INTERNA

Director: Ricardo Gómez Lemus

Teléfono: 56 1260 9340 Ext. 04

Correo: servicios@ogunsolucionesti.com

RECURSOS HUMANOS

Director: Isaac Ulises Carrillo Alarcón

Teléfono: 56 1260 9340 Ext. 05

Correo: servicios@ogunsolucionesti.com

C.2 Canales de Denuncia.

LÍNEA DE INTEGRIDAD

Teléfono: 56 1260 9340 ext. 012

Disponible: 24/7

Idiomas: Español, Inglés

PORTAL WEB

URL: www.ogunsolucionesti.com

Usuario: Registro libre

Acceso: Móvil y escritorio

CORREO ELECTRÓNICO

servicios@ogunsolucionesti.com

Respuesta: Máximo 48 horas

BUZÓN FÍSICO

Ubicación: Lobby principal. Prolongación paseo de la reforma 51 oficina 604 piso 6. Col. Paseo de las Lomas, C. P. 01330, Alvaro Obregón, CDMX.

Recolección: Diaria

Acceso: Solo Oficial de Cumplimiento

C.3 Contactos Externos de Emergencia.

SERVICIOS DE EMERGENCIA

Policía: 911

Bomberos: 911

Cruz Roja: 911

SERVICIOS ESPECIALIZADOS

Asesoría legal externa:

Ricardo Larringa,

Cel. 5519779086

Auditoría forense:

Julio Gómez Silverman,

Cel. 5534649804

Investigación privada:

Cassandra Rivera

Cel. 5564283141