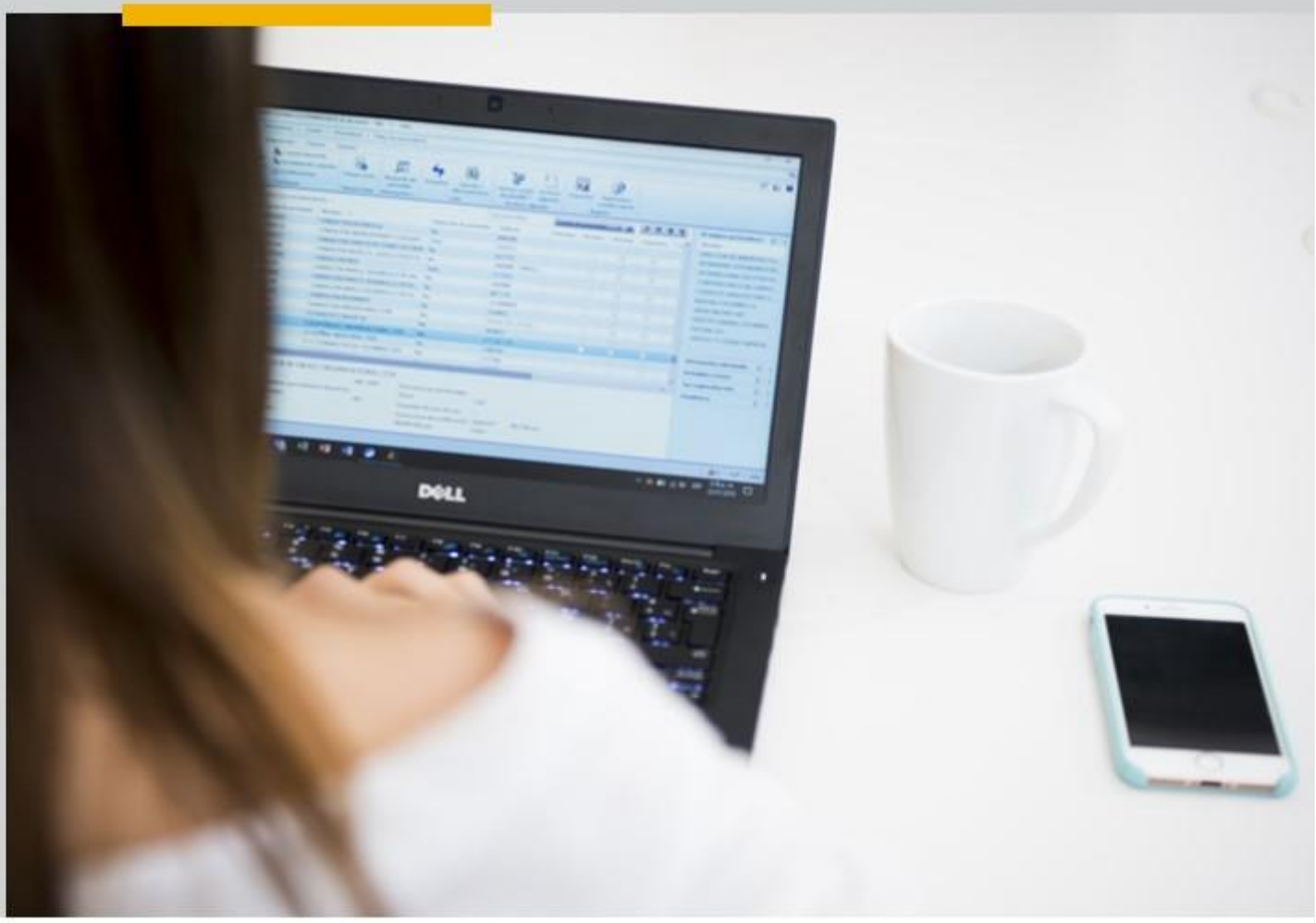

Política de Ciberseguridad

OD-TI-001

ODINSA

Empresa de concesiones del GRUPO ARGOS

CONTENIDO

1. OBJETIVO

Establecer los marcos que orientaran las pautas de comportamiento de colaboradores y terceros involucrados en el manejo de la información y de las operaciones; así como las medidas de protección de las tecnologías que habilitan los negocios. A través de la política se establecen las guías para la implementación de líneas de acción que garanticen la Ciberseguridad de ODINSA y sus compañías vinculadas.

2. ALCANCE

Esta política aplica a todas las geografías en las cuales ODINSA y sus compañías vinculadas tienen operaciones. Adicionalmente, es de obligatorio cumplimiento por parte de todos los colaboradores y todas aquellas personas o entidades que se relacionan con las tecnologías de información y operación de las Compañías.

3. POLÍTICA

POLÍTICA DE CIBERSEGURIDAD

La Compañía en cumplimiento de las leyes y regulaciones para la protección de activos de información[1] físicos, digitales y de ciber activos[2] en los países que operan y en línea con los lineamientos de tecnología; identifica, gestiona y mitiga los riesgos asociados mediante la implementación de las mejores prácticas en ciberseguridad[3] buscando garantizar la confidencialidad, integridad, disponibilidad de la información, tecnologías de información y tecnologías de las operaciones; para asegurar la sostenibilidad de los negocios y la seguridad de las personas.

[1] Activo de información: Conjunto de datos recolectados y transformados que tienen un valor para el negocio de tipo estratégico, operativo, económico, técnico, jurídico o normativo; por ende, su necesidad de protegerlos.

[2] Ciber activo: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

[3] Ciberseguridad: se refiere a la protección de los sistemas informáticos, redes y dispositivos conectados contra amenazas digitales, como el robo de datos, la interrupción del servicio o el acceso no autorizado; mediante el uso de tecnologías, procesos y prácticas adecuadas.

Frente a la ciberseguridad, la compañía, sus colaboradores y terceros que se relacionen con los activos digitales, se comprometen a:

- Asegurar que la política de ciberseguridad está alineada con los objetivos de la compañía y sea un mecanismo para contribuir a la permanencia, sostenibilidad y valor de la organización.
- Apoyar activamente la ciberseguridad dentro de la organización con el fin de dar cumplimiento a las normas en la materia y lograr unos objetivos definidos teniendo en cuenta que la ciberseguridad es una responsabilidad compartida por todos los miembros de la organización.
- Adoptar un enfoque basado en la gestión de riesgos que permita a Odinsa y sus vinculadas y sus colaboradores el libre, seguro y confiable desarrollo de sus actividades en el entorno digital.
- Utilizar toda información almacenada, creada o transmitida usando los recursos de Odinsa y sus vinculadas para uso exclusivo de la organización y el propósito del negocio.
- Mantener un inventario actualizado de los activos de información y los ciber activos existentes con su correspondiente clasificación y propietario.
- Establecer los controles para prevenir la perdida, daño, robo o mal funcionamiento de los activos de información y ciber activos que conlleven a la interrupción de las actividades o afectación de la organización a través de la identificación, evaluación y tratamiento de riesgos, amenazas y vulnerabilidades en sus sistemas de información y operación.
- Asegurar el establecimiento de medidas para el adecuado funcionamiento de su infraestructura tecnológica con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información y los ciber activos, incluyendo las medidas que garantizan la irrenunciabilidad de las acciones de actores internos y externos del entorno digital.
- Comprometer a los colaboradores y terceros que se relacionen en el entorno digital a que conozcan y apliquen los controles para proteger los activos de información y los ciber activos con el fin de reducir el riesgo de errores humanos, robo, fraude o uso inadecuado de los mismos.
- Acceder únicamente a la información relacionada con las funciones de su cargo y responsabilidades. Los terceros que requieren acceso a los sistemas de información solo acceden a la información necesaria para el desarrollo del objeto de sus contratos.
- Difundir y fomentar, de forma planificada, el objetivo de la ciberseguridad, sus características y las responsabilidades individuales para lograrlo, incluyendo planes de capacitación anuales, así como las actividades permanentes y procesos de inducción del nuevo personal.
- Gestionar de forma efectiva los incidentes de ciberseguridad para minimizar el riesgo de pérdida de disponibilidad, confidencialidad, confiabilidad e integridad de los activos de información y ciber activos y para identificar los controles a implementar.
- Asegurar que todos los procesos críticos y los sistemas de información de la

compañía que contengan activos de información tengan planes de continuidad, que aseguren la resiliencia y su recuperación en los tiempos requeridos por el negocio.

- Garantizar que el uso, operación y manejo de los sistemas de información cumplen con los requerimientos de las leyes nacionales e internacionales que aplican, sobre licenciamiento de software, derechos de autor, privacidad de la información, retención de registros de información y todas las disposiciones legales vigentes.
- Respetar la privacidad de los clientes, colaboradores, proveedores, y otros terceros con los que se relacione Odinsa y sus vinculadas y tomar las medidas razonables que garanticen la seguridad de los datos personales que se recolectan, almacenan, procesan, divulgan y transmitan.
- Gestionar con el área de tecnología el desarrollo, adopción o contratación de nuevos aplicativos o servicios tecnológicos, asegurando el cumplimiento de los lineamientos y estándares de ciberseguridad y su correcta integración con el ecosistema de soluciones de la compañía.
- Respetar la política de ciberseguridad o sus lineamientos. Cualquier violación por parte de los colaboradores y terceros que se relacionen con los activos digitales, desencadenarán en medidas de tratamiento a los incidentes de seguridad generados y serán objeto de acciones disciplinarias por parte de las áreas de recursos humanos.
- Garantizar la seguridad de la información y la continuidad de las operaciones, a partir de la investigación del comportamiento digital de los usuarios, por parte de las áreas de control interno y el área de ciberseguridad.

4. GOBIERNO DE CIBERSEGURIDAD

ODINSA y sus compañías vinculadas han definido la siguiente estructura organizacional con instancias, roles y responsabilidades, con el fin de asegurar un adecuado cumplimiento de la política de seguridad de la información y ciberseguridad:

Comité Estratégico de Ciberseguridad:

- Aprobar la estrategia organizacional que proporciona la dirección en la gestión de la seguridad de la información y ciberseguridad.
- Aprobar la política de seguridad de la información y ciberseguridad y sus lineamientos.
- Gestionar el mapa de riesgo de ciberseguridad y evaluar la efectividad de las medidas de tratamiento adoptadas.
- Verificar la adopción de recomendaciones emitidas por entes de control, auditores, compañías de seguros, áreas de riesgos, entre otras.
- Reportar a la junta directiva y la alta dirección.

Miembros:

- Vicepresidencia Administrativa
- Vicepresidencia Finanzas (Riesgos)

- Auditoria o (Cumplimiento)
- Vicepresidencia Aeroportuaria
- Vicepresidencia Concesiones Viales
- Tecnología Summa
- Ciberseguridad

Comité Táctico de Ciberseguridad:

- Proponer lineamientos para materializar la política de ciberseguridad.
- Identificar riesgos y vulnerabilidades del entorno, monitoreando constantemente el ambiente cibernético.
- Supervisar la implementación de medidas de seguridad.
- Proponer el programa de pruebas de intrusión y de simulacros ante ataques cibernéticos.
- Ajustar el programa de capacitación conciencia para todos los miembros de la organización.
- Comunicar y reportar el estado de la ciberseguridad de la organización a la alta gerencia y a otros miembros clave de la organización.

  Miembros:
  - Riesgos
  - Talento Humano (Comunicaciones)
  - Gerencia Operaciones de los Gestores
  - Gestión de Procesos
  - Tecnología Summa
  - Ciberseguridad

Propietarios de activos de información y ciber activos: Responsables de los activos que le sean asignados, así como de la clasificación, control y monitoreo del uso y gestión de estos.

Custodios de activos de información y ciber activos: Responsables dentro de cada compañía de custodiar los activos, haciendo efectivas las restricciones y clasificaciones de acceso dadas por el propietario.

Áreas de Control (Tecnología, Riesgos, Auditoria): Responsables de la gestión y evaluación de las medidas adoptadas para mitigar el riesgo asociado a la ciberseguridad.

Oficial de Ciberseguridad: responsable de desarrollar el modelo de gestión integral de Ciberseguridad; enmarcando la política de ciberseguridad dentro de este ecosistema; a través de la gestión de riesgos asociados a la Seguridad de la Información y Ciberseguridad.

Usuarios: Cualquier colaborador, proveedor, contratista, u otra persona autorizada que utiliza la información de las compañías en la ejecución de las actividades de su trabajo diario.

5. ANEXOS Y REFERENCIAS

- Norma NIST Cybersecurity Framework CSF.
- Normas ISO 27000.
- Leyes y Regulaciones.
- Lineamientos de Seguridad de la información y ciberseguridad y Anexos.
- Política de Tratamiento de Datos Personales.

6. EXCEPCIONES

No aplica

7. PERIODICIDAD DE REVISIÓN DE LA POLÍTICA

Cada año o cada vez que se requiera.

8. APROBACIÓN

Instancia de aprobación: Comité Estratégico de Ciberseguridad
Instancia de revisión: Comité Táctico de Ciberseguridad.

9. CONTROL DE VERSIÓN

Número	Fecha	Descripción del cambio o modificación
1	16/11/2016	Emisión inicial
2	30/08/2023	Instancia de aprobación Comité estratégico de ciberseguridad