Política General de Seguridad de la Información

Elaboró/Actualizó	Revisó	Fecha
David Susa – Desystec SAS		15 de noviembre de 2016

Contenido

1. Justificación y propósito

La información es el activo más valioso en las organizaciones hoy en día. Todos los procesos de negocio tienen como entrada y salida información que es de gran valor para la organización y que debe ser protegida adecuadamente. De esta forma, la seguridad de la información se convierte en un componente esencial para el logro de los objetivos estratégicos de la compañía.

El propósito de esta política es formalizar el compromiso de Odinsa S.A. con el proceso de gestión de la información que tiene como objetivo proteger la información y los activos de información contra amenazas internas o externas, deliberadas o accidentales, con el fin de mantener la integridad, legalidad, oportunidad, disponibilidad y confidencialidad de la información

2. Alcance

La presente política aplica a todo tipo de información objeto de tratamiento dentro de la compañía, incluyendo información en físico y digital; contenida en documentos, archivos, bases de datos, sistemas de información, sistemas de almacenamiento, equipos de cómputo y/o manipuladas por colaboradores y proveedores; es de obligatorio cumplimiento para todos ellos en Odinsa S.A., así como otros terceros que tengan acceso temporal o permanente a información propiedad de la compañía.

3. Definiciones

Activo de información: Se entiende como activo de información cualquier repositorio físico o digital que contenga información relevante para la organización. Como ejemplos se tienen los documentos, el archivo físico, las bases de datos, las aplicaciones, los computadores y las personas. Un activo se clasifica como crítico cuando la pérdida de la confidencialidad, disponibilidad o integridad, afecten significativamente a la organización y su operación.

Amenaza: Se entiende como la posibilidad de la ocurrencia de un evento no deseado, que puede resultar en el daño a un sistema u organización.

Confidencialidad: propiedad de la información que hace referencia a que esta solo debe ser accesible para aquellos individuos que cuenten con los permisos necesarios para hacerlo.

Control: Corresponde a una medida que modifica el nivel de riesgo. Esto incluye procesos, políticas, dispositivos, prácticas o cualquier otra acción que tenga algún impacto sobre las consecuencias o la probabilidad de ocurrencia de un riesgo.

Disponibilidad: propiedad de la información que hace referencia a que esta debe poder ser accedida cuando sea requerida.

Integridad: propiedad que hace referencia a que la información es precisa, completa, inalterada y consistente.

Riesgo: Se refiere a una desviación de lo esperado, positiva o negativa, que genera incertidumbre respecto a su consecuencia o probabilidad de ocurrencia.

4. Objetivos

Odinsa S.A. reconoce que la información que utiliza como parte de su operación es un activo valioso y establece los siguientes objetivos con miras a garantizar su adecuada protección:

- Garantizar la confidencialidad, disponibilidad e integridad de la información de la compañía.
- Implementar en la organización controles técnicos y administrativos que permitan garantizar una adecuada protección frente al panorama de posibles amenazas.
- Generar una cultura de seguridad, en la que todos los colaboradores conozcan los riesgos a los que está expuesta la información en la organización y participen activamente en su protección.
- Establecer en la organización un proceso de mejora continua en torno a la seguridad de los activos de información.
- Cumplir con la legislación aplicable y respetar los derechos de los ciudadanos en torno a su información personal.

5. Política

Los siguientes principios de seguridad definen el marco de gobierno sobre el que se debe gestionar la información en la compañía:

1. **Principio de responsabilidad:** Es deber de cada uno de los colaboradores de la compañía proteger los activos de información que utilizan como parte de sus actividades diarias.
2. **Principio de clasificación:** La información debe ser clasificada y protegida de acuerdo a su importancia para la compañía y considerando los aspectos legislativos, regulatorios y contractuales aplicables.
3. **Principio de uso legítimo:** La información solo debe estar disponible para aquellos que tienen una necesidad legítima de uso y se debe trabajar sobre la base del "menor privilegio".
4. **Principio de aproximación basada en riesgo:** Las estrategias de protección de la información deben estar fundamentadas en un plan de gestión de riesgos, a través del cual se identifican los principales activos de información, potenciales amenazas y fuentes de riesgo, la probabilidad de ocurrencia y su impacto.
5. **Principio de mejora continua:** La seguridad de la información se debe gestionar de forma continua y los responsables dentro de la organización deben garantizar que las estrategias de protección se evalúan periódicamente y se definen acciones de mejora.

Se debe proteger la información siguiendo lo contenido del código de buen gobierno.

- Considerando el carácter técnico de las acciones que debe adoptar cada colaborador se deben observar los lineamientos contenidos en esta política.

Elementos a tener en cuenta:

- Contratos
- Información de cada colaborador – datos de las personas.
- Información relacionada con estrategia corporativa.
- Información hacia afuera.
- Información en relación a las compañías.
- Información asociada a protección de recursos.

5.1 Clasificación de la información

Toda la información de la organización debe ser clasificada dentro de alguno de los niveles o categorías presentados a continuación. A través de la categorización se establecen los requerimientos de seguridad mínimos y los controles que se deben implementar para la adecuada protección de la información.

Los directivos de la compañía y cada uno de los responsables de los activos de información deben asignar una clasificación de acuerdo al estándar presentado a continuación.

CATEGORÍA	DESCRIPCIÓN
INFORMACIÓN PÚBLICA	Esta categoría hace referencia a la información que puede estar disponible y ser conocida por cualquier individuo dentro o fuera de la organización.
INFORMACIÓN INTERNA	Esta categoría hace referencia a la información de uso interno que puede ser conocida por los colaboradores de la organización.
INFORMACIÓN DE RESERVA	Esta categoría hace referencia a la información que es de uso restringido a algún individuo o área dentro de la organización, pues su divulgación indiscriminada puede generar perjuicios a la organización o a terceros.
INFORMACIÓN CONFIDENCIAL	Esta categoría hace referencia a la información de alto valor para la organización y que se debe guardar bajo total reserva porque representa una ventaja estratégica, porque es de naturaleza sensible o porque debe ser protegida atendiendo a obligaciones legales o contractuales. Los datos personales clasificados como privados o sensibles de acuerdo al régimen general de protección de datos personales en Colombia, se clasifican como información confidencial.

5.2 Revelación de información

Compartir o revelar información clasificada bajo las categorías de reserva o confidencial a terceros está prohibido a excepción de los siguientes escenarios: (i) Atendiendo a una necesidad legítima del negocio, para lo cual se debe solicitar autorización de las directivas de la organización y se debe establecer un acuerdo contractual en el que se establezcan los compromisos en torno a la protección de la información; (ii) Atendiendo a un requerimiento judicial o de una entidad de control para una finalidad claramente establecida en la ley.

5.3 Responsabilidades

Miembros de la organización: Dar cumplimiento a las disposiciones contenidas en las políticas de seguridad de la información de la compañía, trabajar para el cumplimiento de los objetivos y respetar los principios allí definidos.

Colaboradores de Odinsa: todos los colaboradores, como parte del proceso de ingreso a la compañía, deben firmar un acuerdo que contenga los términos y condiciones que regulan el uso de la información y las reglas que autorizan el uso de la misma con base en los perfiles necesarios para el desempeño de sus funciones. Los procedimientos para la asignación de tales perfiles, deben ser actualizados y mantenidos por cada área responsable, con la debida aprobación de Auditoría.

Directivos y jefes de área: Dirigir y auditar el cumplimiento de las políticas de seguridad de la información y destinar los recursos apropiados para el cumplimiento de los objetivos estratégicos de la organización en esta materia.

Responsables de activos de información: Clasificar la información, participar activamente en la identificación y gestión de los riesgos y gestionar e implementar los controles técnicos y administrativos establecidos para garantizar la protección de los activos bajo su responsabilidad.

Área jurídica: Documentar los requerimientos normativos y contractuales que aplican a la organización y definir los lineamientos para ajustar la estrategia de seguridad de la información para dar cumplimiento a estos.

Área de tecnología: Gestionar las capacidades técnicas de la organización para garantizar una adecuada protección de los activos de información. Implementar los controles técnicos requeridos de acuerdo a los riesgos identificados.

Terceros, consultores, contratistas y proveedores que administren o manipulen por alguna razón información que sea propiedad de la compañía: todos estos entes deben estar autorizados por un miembro de la organización responsable del control y vigilancia de los activos de información propiedad de la compañía.

Estos usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de la compañía.

Área de Recursos Humanos: debe cumplir con la función de notificar a todo el personal que se vincula a la organización respecto al cumplimiento de la Política de Seguridad de la Información y todos sus lineamientos, por lo tanto debe suscribir compromisos de confidencialidad a dicho personal y contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de los activos de información de la compañía que violen los términos y condiciones establecidos en estos compromisos. Adicionalmente debe, conjuntamente con el área de tecnología, crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información tales como: responsabilidades en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

Área de Auditoría: practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información. Es su responsabilidad informar sobre el cumplimiento de los lineamientos y medidas de seguridad establecidas por la presente política y de los procedimientos y prácticas que surjan de ella.

Comité de seguridad de la información: Dentro de la organización se estructurará un comité de seguridad de la información en el que deben participar funcionarios del nivel directivo de las áreas jurídica, de tecnología, financiera y de operaciones. Este comité tiene como función principal definir y aprobar la estrategia de la organización en torno a la seguridad de la información y establecer los principales lineamientos que guiarán las acciones y proyectos de mejora.

6. Políticas relacionadas

- Política para la protección de datos
- privacidad
- Políticas complementarias de seguridad

7. Revisión y actualización

La presente política debe ser revisada y actualizada como mínimo cada 18 meses o cada vez que exista un cambio importante en la estructura de la organización o en sus objetivos estratégicos.

8. RESPONSABLES DE CONTROL Y APROBACIÓN:

Es responsabilidad de la Dirección de la compañía y del Comité de Seguridad de la Información*, conscientes que la información es uno de los activos más valiosos que posee la compañía, hacer uso de esta Política e incluir como parte del direccionamiento estratégico los lineamientos, reglas de negocio, procedimientos y directrices que garanticen su cumplimiento. Así mismo, garantizar su debida aprobación.

***Comité de Seguridad de la Información:** es responsable de revisar y proponer a la dirección de la compañía para su aprobación, el texto de la Política de Seguridad de la Información.