Guía de Seguridad en el buen uso de Recursos Informáticos

OD-TI-003

ODINSA

Contenido

AUDIENCIA

Esta guía aplica a todo el personal vinculado laboralmente con ODINSA y sus compañías vinculadas, en adelante las Compañías, así como a los contratistas y terceros que tengan acceso a los recursos tecnológicos de las Compañías.

1. OBJETIVO

Establecer las reglas de uso seguro y honesto que deben cumplir los destinatarios de esta norma respecto de los diferentes recursos informáticos y telemáticos dispuestos por las compañías para el desarrollo de su actividad empresarial o los recursos propios de los colaboradores y empleados en los cuales se gestione información de las compañías o entregada a ellas para su custodia.

2. AMBITO DE APLICACIÓN

Las normas contenidas en este documento son de obligatorio cumplimiento por parte de los empleados de las compañías, así como respecto de aquellas personas vinculadas contractual o estatuariamente a ellas.

En caso de que otras entidades, públicas o privadas, hiciesen uso de alguno de los recursos informáticos de las compañías en desarrollo de disposición legal o mandamiento de autoridad competente, o accedieren a la información que circula en tales medios, es obligación advertir por escrito a los funcionarios que las representen y/o cualquiera otro tercero, de la existencia de esta norma con el fin de que las medidas de seguridad de la información aquí contendidas sean adoptadas por tales entidades a efectos de prevenir daños sobre la misma.

3. DERECHOS DE LAS COMPAÑÍAS

Las compañías informan a los destinatarios de esta norma que respecto de los recursos informáticos que adelante se indican, ejerce de manera legal derechos de dominio, derechos de propiedad intelectual y derechos de acceso a redes públicas y/o privadas, y a servicios, en virtud de la existencia de relaciones contractuales con terceros.

Las compañías, adoptan las medidas y controles de seguridad necesarios que aseguren el respeto y protección de tales recursos informáticos.

4. USO HONESTO DE RECURSOS INFORMÁTICOS

Todos los colaboradores y terceros deben conocer y cumplir la **Política de Ciberseguridad**, la cual es de obligatorio cumplimiento.

Toda información almacenada, creada o transmitida utilizando los recursos de la Compañía es relacionada con las funciones de su cargo, es de uso exclusivo y es utilizada para el propósito del negocio. La compañía autoriza las excepciones expresadas

en los numerales posteriores de este documento.

Los colaboradores acceden únicamente a la información relacionada con las funciones de su cargo. Los terceros que requieren acceso a los sistemas de información solo acceden a la información necesaria para el desarrollo del objeto de su contrato.

Se respeta la privacidad de los clientes y se toman medidas razonables que aseguren la seguridad de los datos personales que se recolectan, almacenan, procesan y divulgan.

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.

Las violaciones a la Política de Ciberseguridad o sus lineamientos por parte de los colaboradores desencadenarán en medidas de tratamiento a los incidentes de seguridad generados y serán objeto de acciones disciplinarias por parte de las áreas de gestión humana.

4.1. HARDWARE

4.1.1. Uso del Hardware

Los computadores, servidores y dispositivos periféricos dispuestos y/o entregados por las compañías a los destinatarios de esta norma, para la ejecución de su objeto social tienen como única y exclusiva finalidad que los mismos sean usados para actividades empresariales.

El hardware dispuesto y/o entregado por las compañías debe ser tratado bajo las mejores condiciones de uso, mantenimiento e higiene por parte del colaborador responsable del mismo.

4.1.2. Prohibiciones respecto del Hardware

En virtud de los múltiples riesgos que tiene la información como activo intangible y de los recursos informáticos de las compañías que la almacenan, derivados del malware (software malintencionado que se ha diseñado para ocasionar acciones dañinas en un sistema de información) que puede ser de uso libre o gratuito, deben ser objeto de un análisis de seguridad y del esquema de licenciamiento; una vez aprobados estos análisis por parte del equipo de Tecnologia éste puede ser utilizado, de lo contrario se negará su instalación.

También está prohibido de manera absoluta la instalación de software o programas de ordenador, ofrecidos bajo el régimen de licencia de uso remunerada, cuya titularidad no se haya obtenido a través de las compañías.

Los equipos portátiles de la compañía asignados a un colaborador en ningún caso podrán

ser prestados a terceros, en virtud de la información de las compañías allí contenida.

Los destinatarios de esta norma no podrán variar la configuración del hardware entregado por las compañías, pues tal actividad puede generar una brecha de seguridad en el mismo, siendo de su responsabilidad los daños.

La instalación de software de cifrado en los equipos, sin autorización de las compañías, será tratada disciplinariamente de conformidad con lo determinado para tal efecto.

Se prohíbe la creación y conexión cuando se habiliten redes wifi personal o hotspot, estas pueden generar y comprometer la seguridad de las plataformas y la información de la organización. En razón a lo anterior puede utilizar el wifi de visitantes de las compañías.

4.1.3. Excepciones al uso empresarial del Hardware

De manera excepcional y limitada los destinatarios de esta norma podrán almacenar en el hardware asignado para el desempeño de sus funciones o servicios, archivos de texto relacionados con actividades académicas, información concerniente a su núcleo familiar básico, e información personal concerniente con su patrimonio, siendo toda esta información personal del usuario del hardware y por lo tanto la compañía no es responsable de la perdida de esta.

Las compañías autorizan a los empleados y colaboradores, cualquiera que sea su vinculación con la empresa, para que puedan utilizar su propio hardware representado en equipos móviles, celulares, tabletas, entre otros. Si estos equipos manejan información de la compañía deben aceptar y cumplir las normas y adoptar las recomendaciones de seguridad informática que determine el equipo de tecnología.

4.2. TELÉFONOS MÓVILES INTELIGENTES

Las compañías podrán asignar a los funcionarios, que debido a sus actividades lo requieran, un teléfono inteligente y/o plan de telefonía y de datos y su uso deberá darse según el documento Reglas de negocio de celulares publicado por la compañía.

4.2.1. Prohibiciones respecto del teléfono móvil inteligente y/o los servicios de telefonía o datos suministrados por las compañías

Se prohíbe alterar la configuración de seguridad del teléfono inteligente asignado por las compañías, así como los controles de seguridad de la red, pues tal proceder genera un riesgo la seguridad de los activos de información de las compañías.

4.3. SOFTWARE

4.3.1. Uso del software

En los equipos de cómputo entregados por las compañías solo podrán estar instalados software debidamente licenciados por la misma.

Las compañías informarán y notificarán a los destinatarios de esta norma, al momento de asignársele recursos informáticos para el desarrollo de sus funciones, el inventario de los programas instalados en sus equipos, los cuales serán los únicos que se consideran autorizados para ser utilizados.

Durante la vigencia de la relación contractual, el equipo de tecnología de las compañías monitoreará y verificará que esta disposición se cumpla, con el fin de prevenir violaciones a las normas de propiedad intelectual y/o ataques a sus activos de información provenientes de malware (software malintencionado que se ha diseñado para ocasionar acciones dañinas en un sistema de información) instalado en el hardware.

Los destinatarios de esta norma tienen la obligación de usar el software asignado y/o adquirido para el desempeño de sus funciones conforme las especificaciones de los manuales de usuario y/o técnicos, según aplique. Todo error en las funcionalidades del software será reportado al equipo de Tecnología o mesa de servicio.

El software gratuito que se requiera por la organización en el desarrollo de sus actividades empresariales o se adquiera por los colaboradores de manera autónoma, deberá ser aprobado y autorizado por el equipo de Tecnología.

4.3.2. Prohibiciones respecto del software

Es prohibido hacer copia o reproducción del software entregados por las compañías a los destinatarios de esta norma o adquiridos directamente por los colaboradores, pues tales conductas son violatorias de las normas de propiedad intelectual.

Es contrario a las normas de propiedad intelectual el desarrollo de obras derivadas sin la autorización del titular de la obra original.

Los destinatarios de esta norma no podrán variar la configuración del software autorizado, pues tal actividad puede generar una brecha de seguridad en el mismo y en la estructura de la seguridad informática, siendo de su responsabilidad los daños resultantes de este obrar.

El software instalado y utilizado por el colaborador genera rastros o logs, que pueden ser susceptibles de procedimientos de auditoría.

4.3.3. Excepciones al uso empresarial del software

El software para trabajo de oficina, como procesadores de texto entre otros, de manera excepcional podrán ser usados para actividades académicas y actividades personales básicas. Siendo toda esta información personal del usuario, por lo tanto, la compañía no es responsable de la perdida de la misma.

4.4. INTERNET

4.4.1. Uso de internet

Los destinatarios de esta norma deben usar Internet de manera responsable y siguiendo las medidas de seguridad que disponga el equipo de Tecnología, con el fin de no generar

brechas de seguridad en la información.

Las mismas previsiones de uso honesto establecidas para Internet serán aplicables al uso de la Intranet Empresarial de las compañías.

4.4.2. Prohibiciones respecto de Internet

Es prohibido a los destinatarios de esta norma usar Internet mientras se encuentre prestando sus servicios a las compañías, en dispositivos propios o de la empresa, para acceder a sitios que puedan contener malware o software malicioso como son los sitios de pornografía, juegos, apuestas, subastas, entretenimiento, sitios de descarga o intercambio de software, entre otros.

Como medida de seguridad se prohíbe la transferencia y/o recepción de archivos intercambiados a través de programas gratuitos y/o públicos que no sean autorizados por el equipo de tecnología.

4.4.3. Excepciones respecto de uso empresarial de Internet

Los destinatarios de esta norma podrán hacer el uso de Internet para realizar actividades académicas, actividades concernientes a su núcleo familiar básico y actividades de orden patrimonial en su tiempo de descanso. Así mismo se informa que esta actividad podrá estar sujeta a monitoreo.

4.5. CORREO ELECTRÓNICO

El correo electrónico es una forma de correspondencia, que al igual de la que cursa de forma física, les corresponde a las compañías organizarla, administrarla y preservarla, en cumplimiento de las obligaciones establecidas en la legislación mercantil, respecto de los libros de comercio.

La correspondencia que puede ser generada a través del correo electrónico empresarial hace parte de los libros de comercio de las compañías, adquiriendo en consecuencia el carácter de información reservada, a la luz del Código de Comercio.

4.5.1. Efectos probatorios

La información contenida en el correo electrónico empresarial puede tener el carácter de correspondencia, y por tanto es plena prueba de los negocios empresariales de las compañías y será gestionada conforme las normas comerciales sobre la correspondencia, además tiene plena validez y eficacia probatoria a la luz de la ley 527 de 1999, siempre que cumpla con los atributos de integridad, autenticidad y confidencialidad.

El correo electrónico empresarial y la información en él contenida, podrá constituir evidencia en los incidentes de ciberseguridad que tengan repercusiones jurídicas y/o judiciales.

4.5.2. Medidas tecnológicas

Es propiedad de las compañías toda la información cursada a través del correo electrónico empresarial asignado a los destinatarios de esta norma. Las compañías adoptarán las medidas tecnológicas tendientes a gestionar los correos que impliquen un riesgo para la organización.

Respecto de la información personal de carácter sensible que llegare a identificarse en los contenidos de los correos electrónicos empresariales a través del equipo de Tecnología de las compañías y/o quien ella designe, se procederá a dar aviso al titular del correo electrónico empresarial para que haga el retiro de la misma y disponga de ella.

4.5.3. Finalidad del correo electrónico empresarial

El correo electrónico empresarial es asignado por las compañías a los destinatarios de esta norma con el fin exclusivo de que este recurso sirva como mecanismo de comunicación interno y externo, vinculado a la ejecución de las actividades que componen el giro ordinario de los negocios empresariales.

4.5.4. Riesgos sobre la Intimidad con el uso del correo electrónico

El uso del correo electrónico para los fines personales aquí determinados en todo caso deberá hacerse bajo responsabilidad del destinatario de la presente norma.

No se recomienda a los destinatarios de esta norma exponer información personal ni su privacidad en el correo electrónico empresarial, la exposición voluntaria de esta información constituye una decisión individual y asume las implicaciones de su actuar.

4.5.5. Prohibiciones

La información que se transmita a través del correo electrónico empresarial no podrá vulnerar derechos humanos, ni contener datos contrarios a la moral y las buenas costumbres.

El correo electrónico empresarial es una herramienta de uso individual que no podrá ser cedida a otras personas, siendo de responsabilidad de quien permita su uso cualquier perjuicio que llegare a causar.

4.5.6. Acceso por parte de terceros y de autoridades

Los funcionarios de las ramas jurisdiccionales y ejecutiva del poder público solo podrán acceder al correo electrónico empresarial en los casos establecidos en los artículos 63 y siguientes del Código de Comercio.

Previo el acceso de las autoridades a la correspondencia contenida en el correo electrónico empresarial y de cualquiera otro tercero a quien le asista este derecho de acceso, la Gerencia Legal de Asuntos Societarios de las compañías verificará que el funcionario público y/o dicho tercero tenga la facultad para acceder a tal información. En caso de tener tal facultad, se le notificará la normatividad sobre seguridad de la información y de acceso a la misma que deberá tener en cuenta, a fin de prevenir los riesgos que sobre la misma se cierne.

4.6. MONITOREO, MANTENIMIENTO Y SOPORTE

El equipo de Tecnología realizará labores de monitoreo, mantenimiento y soporte que le permiten acceder a la totalidad de la información almacenada en el hardware o que se transmite a través de la red, así como establecer las actividades que el empleado realiza con base en la trazabilidad de los logs, huellas o rastros generados durante el uso de recursos informáticos. En el ejercicio de esta actividad las compañías actuarán de conformidad con la Norma de Uso de la Información y las demás normas concordantes, reglas y procedimientos que desarrollen la Política de Ciberseguridad.

El equipo de Tecnología informará y eliminará del hardware los programas de ordenador o software instalados que no hayan sido autorizados, en atención a los riesgos de ataques a la información, así como a los riesgos que contra la propiedad intelectual puedan existir.

4.7. AUDITORIA

En cumplimiento con el deber de protección de los activos de información y en desarrollo de las buenas prácticas en materia de ciberseguridad, se requiere desplegar de manera periódica procesos de auditorías en el hardware, software, correos electrónicos, servicios y redes propiedad de la compañía, con el fin de prevenir ataques contra la información, adoptando las decisiones que considere pertinentes para proteger la información de su propiedad o entregada para su custodia.

Las compañías informan a los destinatarios de esta norma que las actividades que se desarrollan a través de tales recursos informáticos dejan unas marcas o huellas (logs) que permiten establecer con precisión las acciones realizadas en términos de tiempo, modo y lugar.

De los resultados de la auditoria la compañía establecerá el cumplimiento de las obligaciones aquí contenidas y definirá las repercusiones jurídicas que pueda tener su incumplimiento; caso en el cual podrá ejercer las acciones legales que considere pertinentes cuando a ello haya lugar.

4.8. ROLES Y RESPONSABILIDADES

Las valoraciones y decisiones respecto del incumplimiento de las obligaciones derivadas de esta norma serán evaluadas por la Gerencia de Talento Humano, de conformidad con el procedimiento sancionatorio vigente.

4.9. EFECTOS DEL INCUMPLIMIENTO

El incumplimiento de esta norma respecto del uso de los recursos informáticos es considerado grave por los riesgos que sobre los activos de la información de las compañías conlleva, sobre los datos de carácter personal que la organización custodia, las creaciones protegidas por la propiedad intelectual, entre otros, y en consecuencia podrá dar lugar a las sanciones disciplinarias que se prevean para tales casos.

4.10. RESTRICCIONES EN EL USO DE ESTA NORMA

Esta norma de protección de datos personales es para uso exclusivo de las compañías, por tanto, está prohibida su copia, reproducción, distribución, cesión, publicación, traducción y cualquiera otro uso por persona distinta a las compañías, en atención al respeto de la propiedad intelectual que ostentan sus creadores, así como por razones de seguridad de la información.

4.11. ACCESOS A LOS SISTEMAS DE INFORMACIÓN

Ningún colaborador puede acceder a una cuenta de usuario que pertenezca a otro colaborador o intentar leer, cambiar o manipular las comunicaciones electrónicas, los archivos o el software de otro empleado sin la autorización de él o de los funcionarios autorizados de la compañía.

4.12. DECLARACIONES PÚBLICAS

Los colaboradores no deben hacer declaraciones sobre la empresa o su posición real o supuesta sobre cualquier asunto a través de foros públicos, como grupos de noticias, tablones de anuncios, web-logs o áreas de chat, excepto las declaraciones con la revisión previa de la compañía y la autorización específica.

4.13. REDES SOCIALES

Para garantizar el cuidado de la reputación e información que se reproduce a través de las redes sociales, es importante que, todos los colaboradores de la compañía tengan en cuenta los siguientes aspectos:

- Los colaboradores no deben utilizar el logotipo de la compañía, así como otra propiedad intelectual, a menos que esté autorizado por el equipo legal de la compañía. Tampoco deben publicar videos, imágenes o cualquier otra reproducción escrita y/o en audio de los espacios físicos, eventos, oficinas, equipos, productos, clientes, proveedores o visitantes de la compañía en los espacios físicos de ésta.

  Sin embargo, de acuerdo con la estrategia definida y teniendo en cuenta la naturaleza de las redes sociales, los colaboradores tendrán una presencia en algunos espacios designados específicamente para ellos, destinados a reforzar el posicionamiento de la compañía. En este caso, los colaboradores pueden publicar fotos o videos de eventos de la compañía en sus propias cuentas personales de redes sociales, siempre que dicho contenido no viole ninguna obligación confidencial, de privacidad, de propiedad de la Compañía o de terceros.

- No utilizar las direcciones de correo electrónico de la compañía para registrarse en redes sociales, blogs u otras herramientas en línea utilizadas para uso personal, a menos que el equipo de Comunicaciones lo autorice previamente por escrito.

- Sin la autorización previa y por escrito de la compañía, los colaboradores no están autorizados para hablar en nombre de la Compañía o declarar que se ha otorgado dicha autorización.

4.13.1. Recomendaciones para la interacción de colaboradores en redes sociales

Los colaboradores de la compañía podrán compartir e interactuar con los contenidos que sean publicados en las redes sociales de la compañía, teniendo en cuenta lo establecido en el Código de Conducta Empresarial y siguiendo estas pautas:

- Los temas internos solo deben discutirse dentro de la compañía, nunca en espacios digitales.
- Sus interacciones con los contenidos sobre la compañía deben caracterizarse por ser respetuosas, transparentes, confiables, oportunas y positivas, evitando en todo momento los comentarios ofensivos.
- En redes sociales siempre habrá discusiones, nada es personal, por lo que los colaboradores deben procurar no entrar en ellas.
- En caso de identificar un posible escenario de crisis en cualquiera de las redes sociales, se recomienda que el colaborador guarde evidencia de la publicación y la envíe en el menor tiempo posible a los integrantes del equipo de Comunicaciones de Odinsa, quienes actuarán de acuerdo con la estrategia y protocolo definidos.
- El colaborador deberá esperar a que sea la marca la que se pronuncie de manera oficial y podrá replicar la respuesta de la marca, pero en ningún momento deberá citar o adjuntar comentarios a título personal.

Los Colaboradores que expresen su opinión sobre asuntos relacionados con los negocios de la Compañía, deben dejar claro a los lectores en cualquier comunicación que discuta o mencione a la Compañía, que las opiniones expresadas son solo del Colaborador y no representan las opiniones de la Compañía.
Abstenerse de hacer declaraciones difamatorias y/o usar lenguaje malicioso, despectivo, vulgar, obsceno, amenazante y/o acosador acerca de la Compañía, sus productos y servicios, compañeros de trabajo, alta dirección, socios, clientes, proveedores y competidores, entre otros.
No publicar información personal identificable o información personal confidencial sobre otros Colaboradores, alta dirección, socios, clientes, proveedores, competidores y/o de terceros, sin el consentimiento previo por escrito de esa persona.
No divulgar ninguna información sobre la Compañía, un cliente o proveedor específico a menos que el equipo Legal haya otorgado una autorización por escrito o dicha información esté disponible públicamente.

Comprobar la configuración de privacidad tanto en el perfil como en los contenidos que se comparten.

Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.

Si tiene alguna inquietud o detecta cualquier actividad sospechosa en los correos

que recibe, en los sistemas de información o un funcionamiento anómalo de su equipo, favor ponerse en contacto con el equipo de Tecnologia por medio de Emma, SOS@odinsa.com o a la extensión 12345.

BIBLIOGRAFÍA

Congreso de la República. (2014). *Ley 1581 de 2014. Por la cual se dictan disposiciones generales para la protección de datos personales.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República. (2014). *Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

ISO International Organization for Standardization. (2013). *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls.*

MinTIC. (2016). *Guía para la gestión y clasificación de activos de información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MinTIC. (2016). *Procedimientos de seguridad de la información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

CONTROL DE VERSIÓN

Número	Fecha	Descripción del cambio o modificación
1	16/11/2016	Emisión inicial
2	11/04/2022	Ajustes oportunidades de mejora en Auditoria del proceso de Ciberseguridad
3	30/08/2023	Instancia de aprobación Comité estratégico de ciberseguridad