POLÍTICAS DE SEGURIDAD DE LA INFORMACION

FECHA DE PUBLICACIÓN: 01/12/2023
DISTRIBUCIÓN: Cualquier sociedad perteneciente a Grupo Indea

Clasificación del documento			
Secreto	Confidencial	Interno	Público ☑

TABLA DE CONTENIDOS

1 Prefacio

1.1 Introducción

Grupo Indea es consciente de la importancia que tiene para su negocio una Política de Seguridad de la Información, ya que se trata de un elemento clave para garantizar la continuidad de las funciones de negocio y la confianza de sus clientes. Adicionalmente, existen condicionantes legales por los cuales Grupo Indea está obligado a realizar una gestión de la seguridad de la información.

La Seguridad de la Información, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la organización en materia de seguridad.

1.2 Objetivos

Las Políticas de Seguridad de la Información de Grupo Indea son una herramienta organizativa, que tiene como objeto concienciar a cada uno de los miembros de la compañía sobre la importancia y sensibilidad de la seguridad de la información y servicios críticos, los cuales permiten a la compañía desarrollarse y mantenerse en su sector de mercado. Adicionalmente, estructura los objetivos de seguridad sobre los activos de la información para su posterior desarrollo de detalle en forma de normas, estándares y procedimientos.

En este contexto, este documento recoge la definición de la política de seguridad como la base para que Grupo Indea pueda operar y tomar decisiones de una forma apropiada en materia de Seguridad de la Información. La presente Política de Seguridad de la Información no dispone de los pormenores para su implementación.

1.3 Alcance

La presente política es de obligado cumplimiento para avalar la seguridad de los procesos de negocio de Grupo Indea y aplica sobre todo el personal interno y externo en sus diferentes ubicaciones (sedes, plantas de fabricación, etc.)

Asimismo, es de aplicación sobre todas las formas intelectuales y físicas de activos de información, incluyendo hardware, software, redes y datos, tanto almacenados y procesados en equipos informáticos como transmitidos por redes, impresos o escritos en papel, remitidos por fax, almacenados en medios legibles digitalmente (p. ej. CD-ROM, cintas, memorias USB…) o verbalizados en conversaciones.

1.4 Marco de Referencia

El marco de referencia de la arquitectura de seguridad de la información está basado en las normas, mejores prácticas y legislación y normativa de referencia aplicable, incluyendo el sector de mercado específico de Grupo Indea.

Entre estas se encuentran:

- ISO/IEC 27002:2013. Código de buenas prácticas para el Control de la Seguridad de la Información.
- ISO/IEC 27001:2013. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
- TISAX® (Trusted Information Security Assessment eXchange) es un procedimiento de prueba e intercambio, común para el sector automotriz.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Reglamento (UE) nº 952/2013 del Parlamento Europeo y del Consejo, de 9 de octubre de 2013, por el que se establece el código aduanero de la Unión
- Reglamento de Ejecución (UE) 2016/481 de la Comisión, de 1 de abril de 2016, que deroga el Reglamento (CEE) nº 2454/93 de la Comisión por el que se fijan determinadas disposiciones de aplicación del Reglamento (CEE) nº 2913/92 del Consejo por el que se establece el código aduanero comunitario.
- Ley 1/1996, de 12 de abril, de Propiedad Intelectual (LPI). Se refiere a un conjunto de normativas legales que protegen los derechos de los creadores sobre sus obras intelectuales.
- La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) es una normativa legal en España, que regula diversos aspectos relacionados con la prestación de servicios en línea, el comercio electrónico y la sociedad de la información. La LSSI-CE fue aprobada para adaptar la legislación española a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, conocida como la Directiva de Comercio Electrónico.

Para dar debido cumplimiento a esta normativa se define la siguiente arquitectura, para los elementos que conforman la Seguridad de la Información de Grupo Indea:

- Política de Seguridad de la Información: define los objetivos de seguridad de la información a través de un conjunto de normas generales de seguridad. La política demuestra el compromiso de Grupo Indea con la seguridad de la información. Debe tomarse como referencia para la toma de todas las decisiones relacionadas con la seguridad.
- Controles de Seguridad de la Información: Los controles de seguridad consisten en un conjunto completo de medidas de seguridad que comprenden prácticas comunes

y son necesarias para implementar la política de seguridad. Las normas de referencia, aunque no únicas y exclusivas, para los controles de seguridad son las ISO/IEC 27002:2013 y TISAX®.

1.5 Excepciones a la política de seguridad

Todos los elementos descritos como "deber" son obligatorios y están relacionados fundamentalmente con requisitos legales o mínimos. Los elementos que se enuncien con el término "deberá" se consideran práctica óptima y se cumplirán. Cuando no se cumpla este "deberá", se tendrán en cuenta las siguientes condiciones:

a) no suponer un riesgo para otras partes de Grupo Indea sus clientes o proveedores;

b) cada usuario es responsable de este incumplimiento, así como transmitir dicho incumplimiento al Comité de Seguridad, ya que es quien debe conocer todo incumplimiento, y sus consecuencias, y proceder a la gestión de los riesgos así introducidos.

1.6 Propiedad, mantenimiento y revisión

El Comité de Dirección de Grupo Indea es propietario de la presente Política de Seguridad de la Información. El Comité de Dirección posee la responsabilidad última del desarrollo, revisión y mantenimiento del documento, así como de la evaluación de su cumplimiento.

El Comité de Seguridad es el propietario por delegación y gestiona la seguridad global con ayuda de los diferentes elementos organizativos de Grupo Indea.

La presente Política de Seguridad de la Información se debe comunicar a través de toda la organización en una forma que sea relevante, accesible y entendible para el lector objetivo.

La presente Política será revisada anualmente o en caso de producirse un cambio a nivel técnico u organizativo que repercuta en los fundamentos de su contenido.

El Comité de Dirección valora positivamente las opiniones, información y demás comentarios relativos a la presente Política. Para ello, Grupo Indea dispone de una dirección de correo electrónico (**security@indea-group.com**) para la recepción de todo tipo de recomendaciones para su mejora.

2 Política de Seguridad de la Información

2.1 Organización

2.1.1 Gestión de la seguridad

Se debe establecer un marco de seguridad para iniciar y controlar la implementación de la seguridad de la información dentro de Grupo Indea. El Comité de Dirección

aprobará y respaldará el desarrollo de acciones en materia de seguridad, las asignaciones de roles de seguridad y la implementación de la seguridad dentro de la compañía.

Se ha establecido un Comité de Seguridad, encargado de la promoción y desarrollo de buenas prácticas de seguridad de la información dentro de la compañía. Este Comité de Seguridad es responsable de proporcionar ayuda a directores, usuarios, personal de TI y otros, a cumplir con sus responsabilidades en material de seguridad de la información.

Los directores de departamento son responsables de la seguridad de la información dentro de sus propias áreas de responsabilidad. Deben tomarse las medidas necesarias para la coordinación de las actividades de seguridad de la información dentro de cada área de negocio.

Grupo Indea se compromete a dar a conocer las obligaciones y requisitos de seguridad que todos los miembros de la organización deben tener en cuenta en el desarrollo de sus funciones.

2.1.2 Cooperación con terceros (proveedores, contratistas)

Los contratos que se suscriban con terceras partes deben incluir una cláusula que establezca que sus empleados cumplirán los estándares, procedimientos y política de seguridad de Grupo Indea.

La dirección responsable del acuerdo con terceros o que disponga de empleados externos garantizará que estos sean informados sobre la política de seguridad de Grupo Indea.

Siempre que cualquier empresa del Grupo Indea formalice un acuerdo con terceros debe realizarse un análisis de riesgos respecto a cuestiones de seguridad. Este análisis del riesgo proporcionará los controles y procedimientos de seguridad.

2.1.3 Externalización de actividades y servicios

La externalización de sistemas de información o procesos de negocio exige un análisis del riesgo. Este análisis proporcionará los controles y procedimientos que, posteriormente, se incluirán en el contrato.

2.1.4 Niveles de seguridad

Se debe desarrollar una política de mínimo privilegio, de forma que los usuarios sólo tengan derecho de acceso a aquellos datos y recursos informáticos, así como a los ficheros con datos personales, que precisen para el desarrollo de sus funciones.

Para tal fin, las aplicaciones deben disponer de diferentes perfiles de usuarios que garanticen la implantación de esta política, debiéndose limitar especialmente el acceso a los ficheros con datos de carácter personal.

2.1.5 Contratos

Las responsabilidades de todas las partes respecto del nivel de seguridad acordado entre Grupo Indea y sus clientes o proveedores, con acceso a los sistemas de información del Grupo Indea, deben describirse en los contratos, y reflejarse en Acuerdos de Nivel de Servicio resultantes antes de formalizar el oportuno contrato.

Asimismo, debe documentarse claramente el nivel de seguridad y los riesgos de seguridad a los que estaría sometida la compañía antes de formalizar los contratos.

Si por necesidades del negocio, el nivel de seguridad a implementar en una determinada situación va a ser inferior al nivel de seguridad básico de Grupo Indea, este escenario se deberá documentar y transmitirlo de forma explícita al Comité de Seguridad. Este mismo escalará al Comité de Dirección dicha situación, para la gestión del riesgo asociado.

El nivel de seguridad a implementar será definido por el Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información (RS.SGSI)

2.2 Gestión de Activos

2.2.1 Propiedad de los activos

Para mantener una protección apropiada de los activos, se deberá inventariar todos los activos principales (hardware, software e información) los cuales han de disponer de un propietario identificado.

2.2.2 Clasificación de la información

Para garantizar que la información reciba un nivel apropiado de protección, la información debe clasificarse conforme al estándar de clasificación de la información de Grupo Indea.

En el proceso de creación de la información, el creador es responsable de su clasificación inmediata. El propietario de la información es responsable de su correcta clasificación y debe revisar la clasificación conforme a los procedimientos de calidad de Grupo Indea, como mínimo una vez al año.

2.2.3 Clasificación de los activos

Grupo Indea realizará una clasificación de los activos (hardware, software e información). Esta clasificación ayudará a la compañía a decidir las medidas de seguridad que puedan necesitarse para determinada información, incluyendo requisitos en caso de contingencia y de recuperación.

2.2.4 Protección de la documentación

La documentación importante de la compañía debe protegerse frente a pérdidas, destrucción y falsificación.

Puede que alguna documentación precise de una conservación segura para cumplir los requisitos legales o normativos, y también para respaldar actividades esenciales de negocio. Ejemplos de este tipo de documentación son aquellos que puedan necesitarse como prueba de que la compañía, que opera dentro de las normas legales o de regulación vigentes, pueda garantizar una adecuada defensa contra posibles acciones legales en su contra; o para confirmar la situación financiera de la compañía respecto de socios, auditores, etc., …

Cuando se elijan medios de almacenamiento electrónico se incluirán procedimientos para garantizar la capacidad de acceso a los datos (legibilidad tanto de los medios como del formato) durante todo el período de conservación, a fin de proteger contra pérdidas derivadas de futuros cambios tecnológicos.

El sistema de almacenamiento y gestión a utilizar garantizará la clara identificación de la documentación y su período legal o normativo de conservación. Deberá permitir, además, la apropiada destrucción al vencimiento de dicho período, si Grupo Indea no los necesitara.

Para cumplir estas obligaciones:

a. Se emitirán directrices sobre la conservación, actualización, almacenamiento, gestión y eliminación de la documentación e información de negocio.

b. Se implementarán controles apropiados para proteger la documentación e información de negocio esenciales frente a pérdidas, destrucción, acceso no autorizado y falsificación.

2.3 Seguridad del personal

2.3.1 Seguridad en el proceso de selección y en las funciones del puesto de trabajo

El proceso de selección de personal puede exigir un análisis previo adicional de la experiencia y referencias del candidato, en función de la naturaleza del puesto que vaya a cubrirse. Este análisis se debe desarrollar con arreglo a la legislación vigente.

Los términos y condiciones de contratación de personal de Grupo Indea deben incluir una cláusula de confidencialidad. Se debe incluir una cláusula adicional que exprese la existencia de la declaración de Política de Seguridad, así como el deber de conocerla y cumplirla.

Los términos y condiciones de trabajo para los contratistas y personal dependiente de éste deben quedar definidos en contratos formales que especifiquen las condiciones necesarias de seguridad, a fin de garantizar el cumplimiento de la Política de Seguridad. Si los contratistas y personal dependiente de éste no se encuentran cubiertos por un contrato entre empresas que contenga una cláusula de confidencialidad, se debe firmar personalmente este tipo de cláusula. El contrato debe

estar formalizado antes de facilitar el acceso a las instalaciones, recursos e información de Grupo Indea.

Deben revisarse las cláusulas de confidencialidad anteriormente mencionadas cuando haya cambios en los términos y condiciones de contratación, a causa de los cuales se produzca una modificación en el nivel de acceso a la información.

Cuando un miembro del personal cause baja en la Compañía, la Dirección de RR.HH. será responsable de garantizar que se lleve a cabo la devolución de todos los bienes propiedad de Grupo INDEA en posesión de la persona que abandona la Compañía, ordenando la cancelación inmediata de los privilegios de acceso, la cual será realizada por el personal del Departamento de I.T.

2.3.2 Formación y concienciación

El personal debe recibir formación periódica, para garantizar el conocimiento de la política, las normas y los estándares de seguridad de Grupo Indea. Asimismo, se debe asegurar que dispone de los recursos necesarios para apoyar la implementación de estas normas en el desarrollo de su trabajo habitual.

2.3.3 Comunicación de las incidencias de seguridad de la información

Las incidencias de seguridad deben ser reportadas lo antes posible al Comité de Seguridad, bien directamente, bien a través de la dirección de departamento correspondiente. Los directores de departamento deben apoyar la implantación de las medidas necesarias para resolver las incidencias de su área.

Todos los miembros del personal deben conocer los procedimientos para la comunicación de incidencias de seguridad según se defina en la organización.

2.3.4 Comunicación de debilidades de seguridad de la información

Los puntos débiles de seguridad deben ser comunicados al Comité de Seguridad, bien directamente, bien a través de la dirección de departamento correspondiente. El Comité de Seguridad, junto con los directores de departamento, son responsables de evaluar el riesgo de seguridad y de tomar las medidas en su área de responsabilidad cuando sea necesario.

Dichos puntos débiles no deben ser puestos a prueba o explotados sin contar con la autorización por escrito del nivel de dirección correspondiente.

2.4 Seguridad física y del entorno

Las áreas de proceso de datos y red de Grupo Indea (por ejemplo, los centros de servidores y otras instalaciones de tecnología de la información) se operan como instalaciones cerradas con acceso controlado exclusivamente para el personal autorizado. El acceso debe estar limitado al personal de Grupo Indea que cuente con una autorización válida.

Se deben aplicar procedimientos especiales para los visitantes, entendiendo éstos como toda persona no autorizada de forma permanente.

Las zonas de carga y entrega especial deben estar controladas y, si fuera posible, aisladas de las zonas de proceso de datos. Las áreas de proceso de datos y red deben estar físicamente protegidas frente a amenazas de seguridad. Asimismo, estas áreas deben ubicarse de forma que se reduzcan los riesgos procedentes de peligros y amenazas ambientales, como daños por fuego y humo, inundación, fallos eléctricos, problemas de humedad, rayos, disfunciones técnicas, sabotaje y robo. Debe determinarse los controles de seguridad y protección que correspondan en función de un análisis de riesgos.

Se debe realizar un mantenimiento del equipamiento con arreglo a los procedimientos documentados por los proveedores a fin de garantizar su disponibilidad continua.

El acceso a información sensible en medios legibles mecánica o digitalmente, o en papel, debe protegerse mediante los controles apropiados. La información sensible no debe dejarse donde pueda ser accesible por personal que no esté autorizado a hacerlo.

Los ordenadores de sobremesa y portátiles deben contar con medidas de seguridad que eviten el acceso o manipulación no autorizados (por ejemplo, salvapantallas protegidos por contraseña, uso de candados de seguridad, etc.). Esto también es aplicable a otros equipos electrónicos portátiles (por ejemplo, PDAs, teléfonos móviles, etc.).

Cuando se eliminen equipos o medios que contengan información sensible, el proceso debe garantizar que posteriormente no se pueda recuperar la información.

2.5 Seguridad de la red

2.5.1 Redes

La red interna corporativa de Grupo Indea está compuesta por las subredes que contienen a todo el personal y recursos internos que soportan los procesos de negocio de Grupo Indea. Debe ser accesible exclusivamente por el personal y los subcontratistas autorizados de Grupo Indea. Debe realizarse una segregación de la red interna en diferentes subredes en base a las funciones de los servicios proporcionados por los diferentes elementos de red y el uso de estos.

Es obligatorio el control de las conexiones externas a la red. El control de las conexiones de red externas debe ser proporcionado por la propia red (por ejemplo, mediante “firewalls”, “gateways” o “listas de control de acceso”) y debe cumplir los estándares de Grupo Indea.

Quedan prohibidas todas las prácticas intencionadas que hagan peligrar la seguridad de la red de Grupo Indea.

El personal de Grupo Indea no tiene permitido intentar realizar ningún tipo de acceso no autorizado ni uso de sistemas o redes internas de Grupo Indea, de clientes o proveedores. Tampoco se permite realizar ningún tipo de acceso no autorizado ni uso de sistemas o redes externos de terceros, mediante el uso de recursos informáticos de Grupo Indea, propios, de clientes o proveedores.

Sólo se permite el software y las herramientas estándar aprobadas por Grupo Indea en los ordenadores y redes de Grupo Indea.

El personal de Grupo Indea no tiene permitido instalar ningún tipo de herramienta de "hacking" en la red y/o puestos de trabajo de Grupo Indea, salvo que esté expresamente autorizado por la Dirección y bajo el conocimiento y la supervisión del Comité de Seguridad con arreglo a las directrices de seguridad. Estas herramientas deben ser autorizadas de manera individual y no ser compartidas con nadie más.

2.5.2 Conexiones públicas a Internet

Todas las conexiones entre las redes del Grupo Indea e Internet (o cualquier otra red pública) para acceder a servicios de red deben incluir una arquitectura de cortafuegos para filtrar el tráfico y bloquear el acceso no autorizado. Todo el tráfico entrante y saliente debe pasar por este cortafuegos. Se permite únicamente el paso a través de este cortafuegos a los servicios de red respecto de los cuales haya una necesidad. Todos los cortafuegos deben configurarse y gestionarse para asegurar el cumplimiento de los requisitos de seguridad.

El establecimiento de una conexión directa entre los sistemas informáticos de la compañía y los sistemas informáticos de organizaciones externas, a través de Internet o de otra red pública, debe contar con autenticación fuerte y cifrado del tráfico en función de la clasificación de la información del Grupo Indea.

2.5.3 Conexiones de terceros

Las redes de terceros no deben conectarse directamente a las redes del Grupo Indea. Todas las conexiones entre las redes del Grupo Indea y las redes de terceros deben efectuarse por una pasarela segura para filtrar el tráfico / protocolos y bloquear el acceso no autorizado. Todo el tráfico entre las redes de la compañía y la red de terceros (de entrada y salida) debe pasar por esta pasarela. Cualquier conexión entre las redes del Grupo Indea y redes de terceros requiere un análisis de riesgos.

Los requisitos de seguridad del Grupo Indea deben incorporarse en los contratos con terceros con los que se establezca la conexión, definiendo las responsabilidades del Grupo Indea y de la compañía externa.

2.5.4 Acceso remoto

El acceso remoto a las redes del Grupo Indea se facilitará según "necesidad de negocio", a discreción del director del departamento. El acceso remoto debe estar restringido a los miembros autorizados del personal.

El personal autorizado que utilice servicios de acceso remoto debe proteger adecuadamente su puesto de trabajo para evitar el acceso no autorizado a la red del Grupo Indea. Es personalmente responsable de la protección de su puesto de trabajo y del uso correcto del servicio de acceso remoto. Asimismo, no está permitido conectarse a ninguna otra red (vía módem, WiFi, ADSL u otra conectividad) en un puesto de trabajo mientras dicho puesto de trabajo esté conectado a las redes de la compañía (incluida la Red de Área Local).

El servicio de acceso remoto mediante VPN debe estar configurado para asegurar que todo el tráfico desde y hacia el PC sea enrutado a través de la VPN, previniendo, por tanto, que haya conexión simultánea con cualquier otra red. Además, el puesto de trabajo utilizado (ordenador de sobremesa o portátil) debe contar con la última versión y actualización de la herramienta estándar de Grupo Indea utilizada para la protección ante software malicioso o dañino. Estas herramientas deben, asimismo, tener constantemente habilitada la monitorización.

2.6 Seguridad de sistemas

Los empleados del Grupo Indea son personalmente responsables de la protección de su puesto de trabajo (ordenador de sobremesa, portátil y otros dispositivos) en todo momento.

Todos los puestos de trabajo (ordenadores de sobremesa, portátiles) deben estar equipados con un cortafuegos personal y/o software de detección/protección frente a intrusión, y con las medidas de seguridad estándar contra software malicioso o dañino. Son obligatorias las actualizaciones periódicas de seguridad (parches de seguridad) de sistemas y aplicaciones.

2.6.1 Identificación y autenticación

Los usuarios de los sistemas del Grupo Indea están obligados a identificarse de forma unívoca. El método estándar utilizado es la identificación mediante el uso de un ID personal de Usuario, y autenticación adicional a través, como mínimo, de una contraseña con un criterio de complejidad. Los usuarios deben mantener su contraseña en secreto, cambiarla regularmente, no deben almacenarla en su ordenador personal sin utilizar archivos cifrados, y no deben intentar descubrir las contraseñas pertenecientes a los demás.

No se permite el uso de identificaciones funcionales ni compartidos. Pueden permitirse excepciones a esta última restricción siempre que se establezcan los

procedimientos adecuados para un acceso controlado a dichas cuentas funcionales o compartidas.

El proceso de gestión de los sistemas debe poseer un procedimiento para restablecer las contraseñas, que incluya las acciones necesarias para la identificación positiva del solicitante. El usuario debe cambiar su contraseña inicial inmediatamente.

Los usuarios deben cumplir la Política de Contraseñas del Grupo Indea y los sistemas de la compañía implementarán y exigirán dicha Política de Contraseñas, la cual define la complejidad mínima de la contraseña, periodo de caducidad/renovación, bloqueo de cuenta o aplicación e histórico de contraseñas a comprobar para evitar repetir una contraseña anterior reciente.

La identificación y autenticación se consiguen a través de una solicitud de entrada o acceso (login) dependiente de la plataforma y/o sistema. Este procedimiento de entrada debe proporcionar información mínima sobre el sistema, a fin de evitar facilitar ayuda innecesaria a un usuario no autorizado. Durante el proceso de acceso a un sistema, no se deben entregar al usuario información específica que indique la fuente del problema, si una parte de la secuencia de entrada es incorrecta. Solamente se debe informar al usuario de que el proceso de entrada ha sido incorrecto.

Cuando no sea posible técnica o funcionalmente la identificación del usuario; por ejemplo, el acceso a través de una red pública o la comunicación directa de aplicación a aplicación, deben tomarse medidas adicionales. Estas medidas incluyen el enrutamiento forzado a servicios o aplicaciones predefinidos a través de pasarelas de red o aplicaciones de confianza.

Adicionalmente, debe valorar la posibilidad de establecer restricciones sobre los tiempos de conexión para determinados usuarios en sistemas sensibles o críticos. También debe valorarse un sistema de usuario con desconexión automática que se active automáticamente tras un período de inactividad.

2.6.2 Control de Acceso y Autorización

Debe existir un proceso formal de autorización para conceder el acceso a los sistemas. El acceso al sistema debe adjudicarse en función de la "necesidad de usarlo". El uso de "privilegios del sistema" o de utilidades del sistema debe estar restringido al personal de gestión del sistema.

Es necesario el control de acceso para los sistemas y los datos que se compartan con otros. El propietario de la información en un sistema compartido es responsable de decidir a quién se permite acceder y qué autorizaciones se otorgan.

Debe prestarse especial atención a las carpetas compartidas en red y todo sistema de gestión documental presente en la compañía.

2.6.3 Administración de la seguridad

Debe existir un procedimiento de registro de usuario para incorporar nuevos usuarios en un sistema. Sólo podrán implementarse las peticiones aprobadas por el propietario de la información en ese sistema. Debe estar disponible un registro de todos los usuarios inscritos para el uso del sistema.

Debe existir un proceso para bloquear o borrar una identificación de usuario tras la notificación. Cuando un usuario cause baja en la compañía, la Dirección de Recursos Humanos es responsable de notificarlo a responsable de seguridad de los sistemas de información.

Debe existir un proceso para revisar los derechos de acceso de los usuarios como mínimo trimestralmente.

2.6.4 Gestión del sistema

Todas las identificaciones o cuentas estándar del sistema que no sean necesarias deben ser eliminadas del mismo. Cuando se precise una identificación estándar del sistema, deberá cambiarse la contraseña por defecto proporcionada por el proveedor.

Los entornos de desarrollo y pruebas deben estar segregados de los sistemas operacionales o de producción.

Los procedimientos operativos documentados deben estar disponibles para todos los sistemas de producción, a fin de garantizar su correcto funcionamiento. Los cambios en los sistemas deben estar estrictamente controlados por el uso de procedimientos documentados de control de cambios. Los administradores de los sistemas deben garantizar que se establezcan mecanismos de marcha atrás apropiadas en función de la criticidad para el negocio.

Los requisitos de capacidad deben ser monitorizados y deben realizarse previsiones de capacidad a fin de garantizar que se disponga de capacidad adecuada de procesamiento y almacenamiento cuando sea necesario.

2.6.5 Registro, supervisión, comunicación y auditoría

Debe mantenerse un registro de los eventos y actividades relacionados con la seguridad.

Los directores y administradores del Sistema deben impulsar la realización de auditorías regulares para garantizar que se mantenga la confidencialidad, integridad, disponibilidad y capacidad de auditoría de los Sistemas.

2.6.6 Copia de seguridad y recuperación

Se deben facilitar servicios adecuados de copia de seguridad, en función de la importancia o valor de la información, a fin de garantizar que el software de los sistemas, el software de las aplicaciones y los datos puedan recuperarse tras un fallo del sistema o de los medios de almacenamiento.

Los archivos de copia de seguridad deben almacenarse en un emplazamiento remoto, a suficiente distancia del emplazamiento principal, de forma que se eliminen riesgos comunes a ambas ubicaciones, y deben contar con un nivel apropiado de protección física, en coherencia con la seguridad física del emplazamiento principal.

Debe comprobarse regularmente los procesos de copia de seguridad y restauración.

2.6.7 Protección ante software malicioso o dañino

Todos los puestos de trabajo del Grupo Indea deben estar protegidos contra software malicioso o dañino mediante el uso de las herramientas estándar de la compañía. Todos los servidores conectados con puestos de trabajo, o conectados a un entorno no protegido, deben ejecutar este tipo de herramientas. El software de protección debe mantenerse actualizado y estar permanentemente habilitado, monitorizando constantemente en busca de software malicioso o dañino y su actividad relacionada. Los archivos de firma deben actualizarse como mínimo una vez por semana.

Todo el software y todos los archivos de datos nuevos, especialmente si estos archivos proceden de fuentes desconocidas o carentes de confianza (como Internet), o dispositivos no protegidos como dispositivos de almacenamiento externos, deben ser escaneados en busca de software malicioso o dañino antes de su uso. Antes de la distribución de software o archivos de datos a un tercero, estos deberán ser igualmente escaneados.

Si se detecta software malicioso o dañino y el software de protección no puede limpiarlo automáticamente, deberá informarse inmediatamente a la organización de soporte.

El personal del Grupo Indea no deberá escribir, generar, propagar, ejecutar ni intentar introducir jamás intencionadamente ningún software malicioso o dañino dentro de los sistemas de la compañía o Internet.

Los equipos informáticos no pertenecientes al Grupo Indea, utilizados por cualquier tipo de personal por motivos de trabajo, deben estar protegidos contra código malicioso o dañino mediante el uso del software de protección aprobado del Grupo Indea. Se debe escanear sus archivos de datos antes de utilizar estos archivos dentro del entorno de la compañía.

2.6.8 Informática móvil y teletrabajo

Los empleados del Grupo Indea son personalmente responsables de la protección de su ordenador portátil cuando estén fuera de las instalaciones de la compañía. No deben dejarse sin atender los ordenadores portátiles en lugares públicos.

El personal del Grupo Indea es responsable de la protección de los activos de la compañía (hardware, software e información) y debe tomar todas las precauciones que resulten razonables para proteger los activos de las empresas del grupo en

cumplimiento de la política de seguridad, incluyendo la protección mediante contraseña de dispositivos móviles y el cifrado de datos con información confidencial.

2.6.9 Seguridad de los puestos de trabajo

Sólo se consideran seguros los puestos de trabajo pertenecientes a los activos del Grupo Indea y sólo estos pueden utilizarse para todo tipo de actividad autorizada en las redes de la compañía, mientras se manipule cualquier tipo de datos clasificados.

Los visitantes externos al Grupo Indea no tienen permitido conectar sus equipos a las redes de la compañía, y cada empleado que reciba visitantes debe hacer cumplir esta directiva.

Cuando viaje fuera de la oficina local, se recomienda al personal del Grupo Indea que limite el uso de los puestos de trabajo que conforman los activos del grupo para la manipulación de datos de los que la compañía sea responsable y para la conexión a las redes de del Grupo Indea.

2.7 Seguridad de aplicaciones y datos

Se deben valorar detenidamente los requisitos de seguridad antes de desarrollar, cambiar o elegir una aplicación.

Asimismo, se debe comprobar el cumplimiento de los requisitos de seguridad de las aplicaciones previamente a su puesta en producción.

Se deben crear entornos distintos para distintas actividades durante el ciclo de vida de una aplicación; es decir, durante el desarrollo, pruebas y producción. Debe existir una segregación entre estos entornos a fin de evitar que los datos de los entornos de pruebas y desarrollo se utilicen en el entorno de producción. No debe utilizarse datos reales de producción en el entorno de pruebas o para probar las aplicaciones.

Debe haber un estricto control de acceso de todos los entornos.

2.7.1 Aplicaciones Grupo Indea

Deben determinarse y documentarse los requisitos de seguridad en un plan de seguridad antes de que se diseñe y desarrolle o adquiera una aplicación.

Se prestará atención específica a las siguientes áreas de riesgo:

- ✓ Acceso a la aplicación, funciones y datos.
- ✓ Almacenamiento de datos.
- ✓ Transporte de datos.
- ✓ Interfaces con otras aplicaciones.
- ✓ Capacidad de control y trazabilidad (por ejemplo, rastros para auditoría).

Todas las aplicaciones deben comprobarse y aceptarse antes de llevarse a producción. Durante la prueba de aceptación de nuevas aplicaciones desarrolladas o adquiridas debe realizarse una comprobación del cumplimiento de los requisitos de seguridad. También debe comprobarse los requisitos de seguridad cuando las aplicaciones se modifiquen posteriormente.

Debe existir un control estricto de acceso para todos los entornos. Cuando sean operativas, debe hacerse cumplir todas las medidas de seguridad necesarias, tanto manuales como automatizadas. Los cambios que afecten a las aplicaciones deben controlarse de forma estricta mediante el uso de procedimientos documentados de control de cambios.

Deben considerarse controles especiales cuando las aplicaciones inicien procesos críticos de negocio que conlleven la gestión o intercambio de información sensible.

2.7.2 Servicios online

La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje. Asimismo, debe cumplirse cualquier normativa relacionada con la protección de información personal.

Toda aplicación o servicio online debe ser revisado en base a las normativas de seguridad y legislación vigente sobre comercio electrónico de Grupo Indea previamente a su desarrollo e implantación.

2.8 Servicios de información corporativos

2.8.1 Correo electrónico

El personal del Grupo Indea debe ser consciente de que los mensajes electrónicos podrían ser reenviados, interceptados, impresos y almacenados por otros. El personal debe abstenerse de enviar información sensible por correo electrónico salvo que el mensaje esté cifrado.

El emisor de un mensaje electrónico es personalmente responsable de su contenido. Todo el correo debe ser redactado y enviado de manera profesional, siguiendo todas las normas de decoro social que correspondan. Por consiguiente, el personal debe abstenerse de enviar mensajes que pudieran ser considerados discriminatorios, difamatorios, ofensivos o ilegales.

Reconociendo que alguna información está destinada a determinadas personas y puede que no sea adecuada para su distribución general, en las comunicaciones electrónicas, el personal debe tener precaución al reenviar mensajes. No debe reenviarse información sensible a ninguna persona ajena a la compañía sin contar con

el consentimiento previo del propietario de la información. No se permite el reenvío automático de mensajes a personas ajenas al Grupo Indea.

El correo electrónico no deseado o spam y el correo electrónico que contenga contenido ilegal o malicioso se considera inaceptable. Al visitar sitios web y tener que cumplimentar información por cualquier motivo, el personal debe tener cuidado antes de usar su dirección de correo electrónico corporativa, ya que podría tener como resultado la recepción de correo electrónico comercial no solicitado ni deseado. Por ello, el personal debe abstenerse de dejar su dirección de correo corporativa si el sitio web carece de política de privacidad o si ésta manifiesta que la información se traspasará.

El Grupo Indea respetará la privacidad de sus usuarios de correo electrónico. Normalmente, los usuarios del correo electrónico pueden dar por hecho que sólo el destinatario lee su correspondencia electrónica. Sin embargo, puede que se solicite el acceso a los buzones de correo electrónico de los usuarios en caso de urgencia de negocio, incluidas las actividades de investigación. Puede que también sea necesario que el personal de soporte técnico revise el contenido de las comunicaciones de un miembro del personal durante la resolución de un problema. El personal de soporte técnico no debe revisar el contenido de las comunicaciones que no vayan dirigidas a ellos.

Todas las acciones aquí mencionadas deben cumplir la legislación vigente de aplicación.

2.8.4 Web pública externa

La integridad de la información debe protegerse evitando la modificación no autorizada. Deben tomarse las medidas de protección necesarias para el mantenimiento de la disponibilidad de la información y del servicio ofrecido a través de las Webs públicas de Grupo Indea.

2.9 Gestión de la continuidad del negocio

Cada elemento organizativo del Grupo Indea debe evaluar los riesgos para la continuidad del negocio ante un posible desastre respecto de sus actividades críticas de negocio. Deben desarrollarse planes de continuidad del negocio para proporcionar protección contra la pérdida de activos (personas, hardware, software, ubicaciones, proveedores e información). Estos planes deben garantizar que cada posible desastre que plantee un riesgo no aceptable esté adecuadamente cubierto mediante un plan completamente documentado y probado, de forma que el impacto se minimice y puedan retomarse lo antes posible las actividades interrumpidas.

Para garantizar que la infraestructura tecnológica de Grupo Indea siga prestando sus servicios, los directores de departamento responsables de los componentes de dicha

infraestructura deben mantener un plan de continuidad del negocio que pueda implementarse si un desastre impide la prestación normal del servicio.

Los planes de continuidad de negocio deben ser capaces de proporcionar los requisitos de disponibilidad y deben ser comprobados al menos una vez al año y auditados.

Los requisitos sobre continuidad del negocio deben incorporarse a los acuerdos con proveedores que se identifiquen como necesarias para el soporte a las actividades críticas de Grupo Indea y describirse en los contratos y Acuerdos de Nivel de Servicio.

2.10 Cumplimiento

2.10.1 Cumplimiento de la política de seguridad

El diseño, funcionamiento y uso de cada instalación, red, sistema, aplicación y su información debe cumplir la política de seguridad del Grupo Indea, los acuerdos contractuales, la normativa pertinente y demás requisitos.

2.10.2 Cumplimiento de los requisitos legales y regulatorios

El uso de copias ilegales y carentes de licencia de software comercialmente disponible constituye un delito por el que se puede procesar a la compañía. El Grupo Indea debe adquirir suficientes licencias de software y prohibir el uso de software no autorizado. En esta línea, la compañía debe comunicar a los empleados que está prohibida la instalación de software personal o ajeno a la compañía.

2.10.3 Comprobación del cumplimiento

El cumplimiento de esta política y posteriores estándares y procedimientos de seguridad dentro de una organización será revisado bajo la responsabilidad del Comité de Seguridad. Los incumplimientos se comunicarán a la dirección responsable y al Comité de Dirección. Los directores de departamento deben garantizar y facilitar la toma de medidas puntuales, apropiadas y auditables para resolver los incumplimientos.

2.10.4 Consecuencias del incumplimiento

El incumplimiento por parte del personal de Grupo INDEA de las obligaciones establecidas en la Política de Seguridad de la Información y su normativa de desarrollo, será considerado como falta laboral.

3 Declaración de la Política de Seguridad de la Información

3.1 Introducción

Grupo Indea considera la información como un activo estratégico, y como tal, debe ser protegido adecuadamente para garantizar el desarrollo de su modelo de negocio y mantener la confianza de sus clientes. Adicionalmente, existen obligaciones legales y normativas por las cuales la compañía debe realizar una gestión apropiada de la seguridad de la información.

En este contexto, Grupo Indea es consciente de la importancia que tiene establecer un marco de referencia que defina los objetivos de seguridad y las directrices de actuación para garantizar que la integridad[1], confidencialidad[2] y disponibilidad[3] de su información y la de sus clientes no pueda verse comprometida.

La Política de Seguridad de la Información de Grupo Indea constituye el marco normativo de referencia orientado a la definición, gestión, administración e implantación de las medidas de seguridad necesarias para alcanzar el nivel de seguridad adecuado en los activos de información de la compañía.

3.2 Objetivos

La Política de Seguridad de la información pretende garantizar que:

- ✓ Se realiza una gestión del riesgo continua y adecuada sobre los activos de información.
- ✓ Se asegura la confidencialidad de la información.
- ✓ Se mantiene la integridad de la información.
- ✓ Se cumplen los requisitos de disponibilidad marcados por las necesidades de negocio.
- ✓ Se establece una política de clasificación de activos de la información.
- ✓ Se cumple con la legislación vigente en materia de seguridad de la información.
- ✓ Se realiza una formación continua del personal en materia de seguridad de la información.

3.3 Alcance

La presente Política de Seguridad de la Información aplica a todo el personal de Grupo Indea, así como a sus contratistas y empleados de éstos, con acceso a activos de información

[1] Protección de la información frente a modificaciones no autorizadas.

[2] Protección de la información frente a accesos no autorizados.

[3] Protección de la información para garantizar el acceso autorizado a la misma, en el instante necesario.

corporativos, independientemente de su ubicación. Asimismo, es de aplicación sobre todas las formas intelectuales y físicas de activos de información.

3.4 Responsabilidades

El Comité de Dirección es el propietario de la Política de Seguridad de la Información, y por tanto, aprueba la normativa de seguridad asociada, así como las posibles excepciones a la misma. Además, proporciona los recursos necesarios para la implantación de las medidas de seguridad necesarias en la compañía.

El Comité de Seguridad de la Información asume la responsabilidad sobre la planificación, implantación, mantenimiento y mejora de los controles y medidas de seguridad que se establezcan. Además, proporcionará el asesoramiento y orientación necesarios al resto de la compañía y promoverá las acciones continuas de comunicación y formación a todos los empleados en materia de seguridad.

Los directores de departamento son responsables de hacer efectiva la Política de Seguridad de la Información dentro de sus propias áreas de responsabilidad.

Todos los miembros de la organización ayudarán a la generación de procedimientos, guías y al establecimiento de buenas prácticas en su ámbito de actuación, de forma que se desarrolle un marco documental apropiado que dé soporte al cumplimiento de la Política de Seguridad.

Cada empleado y persona relacionada con la organización debe cumplir la Política de Seguridad, así como la normativa, estándares y procedimientos asociados. Existe, además, la obligación de informar de cualquier incumplimiento o incidencia en materia de seguridad de la información, según el procedimiento de gestión de incidencias establecido.

El incumplimiento por parte del personal de Grupo Indea de las obligaciones establecidas en la Política de Seguridad de la Información y su normativa de desarrollo, podrá considerarse falta laboral y será corregido con las medidas disciplinarias establecidas por la legislación vigente y el convenio colectivo aplicable.

3.5 Objetivos de Seguridad

La Seguridad de la Información, es una función en la que se deben evaluar y administrar los riesgos asociados a los activos de información. En este sentido, la Política de Seguridad de la Información se estructura según unos objetivos generales que, en definitiva, definen el nivel seguridad y de riesgo aceptado por la compañía.
Estos objetivos de seguridad se agrupan en los siguientes elementos dentro de la Política de Seguridad:

- ✓ Organización de la seguridad.
- ✓ Gestión de los activos de información.
- ✓ Seguridad relacionada con el personal.

- ✓ Seguridad física y del entorno.
- ✓ Seguridad de la red, comunicaciones, sistemas, aplicaciones y datos.
- ✓ Gestión de la continuidad de negocio.
- ✓ Cumplimiento legal y normativo.

3.6 Comunicación

La Política de Seguridad de la Información y su normativa de desarrollo deben comunicarse a través de toda la organización en una forma que sea relevante, accesible y entendible para el lector objetivo.

El Comité de Seguridad está a disposición de todo el personal para cualquier consulta o comentario que desee realizar, a través de la dirección de correo electrónico **security@indea-group.com**

Elaborado por:	Revisado por:	Aprobado por:
Miguel J. Vázquez Caride **CIO** Fecha: 01/12/2023	**Jose Antonio San Juan** **Arturo Diéguez** **Rocío Arribas** **TIC** Fecha: 01/12/2023	**Javier Echauri** **CEO** Fecha: 01/12/2023