POLITICA DE SEGURIDAD DE LA INFORMACION

INDEA INGENIERIA DE APLICACIONES S.L

IVAC INSTITUTO DE CERTIFICACIÓN

Indea
ingeniería de aplicaciones

entidad certificada

INDEA INGENIERÍA DE APLICACIONES, S.L.

norma de evaluación

ISO 27001:2007

número de certificado

007/2013

periodo de validez

Desde el 09/08/2013
hasta el 08/08/2016

IVAC INSTITUTO DE CERTIFICACIÓN

Miguel Angel Vila Espeso
Director

Este certificado carece de validez si la entidad no figura inscrita en el "Registro de Entidades Certificadas" del IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. (http://www.ivac.es) y en su anexo técnico, cuyo número coincide con el de este certificado y donde queda definido el alcance.
Cualquier aclaración sobre este documento se puede solicitar por escrito al IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.

❖ POLITICA DE SEGURIDAD DE LA INFORMACIÓN INDEA

En INDEA, consideramos que la información es un activo fundamental para la prestación de nuestros servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una gestión segura de toda la información que trata la organización.

Consciente de sus necesidades actuales, INDEA implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales y regulatorios con cada uno de nuestros clientes, proveedores, etc.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en INDEA; este proceso será liderado de manera permanente por el responsable de seguridad de la información en INDEA.

Esta política será revisada con regularidad o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

➢ POLITICAS GENERALES DE LA SEGURIDAD DE LA INFORMACION

INDEA ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1.Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de INDEA.

2.Los activos de información de INDEA, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3.INDEA definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.

4.Todos y cada uno de los empleados de INDEA, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5.Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de INDEA.

➢ ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados de INDEA y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de INDEA a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

➢ RIESGOS RELACIONADOS CON TERCEROS

INDEA identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

➢ USO ADECUADO DE LOS ACTIVOS

Todos los empleados de INDEA que manipulen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerado como un “incidente de seguridad”.

Con las actividades propias del negocio de INDEA, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

•El acceso a páginas que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

•El intercambio no autorizado de información de propiedad de INDEA, de sus clientes y/o de sus funcionarios, con terceros.

b) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

➢ CORREO ELECTRONICO

Los empleados y terceros autorizados a quienes INDEA les asigne una cuenta de correo deberán seguir los siguientes procedimientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del INDEA, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de los usuarios de INDEA y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el departamento de informática de INDEA

➢ CONTROL ACCESO FISICO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

➢ PROTECCION Y UBICACION DE LOS EQUIPOS

Los equipos que hacen parte de la infraestructura tecnológica de INDEA tales como, servidores, equipos ofimáticos y seguridad electrónica, dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información , deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, entre otros.

➢ PROTECCION CONTRA SOFTWARE MALICIOSO

INDEA establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso. Será responsabilidad del departamento de informática, autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, INDEA define los siguientes procedimientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente instaladas por INDEA.

➢ COPIAS DE RESPALDO/ SEGURIDAD

INDEA debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el departamento de informática y las dependencias responsables de la misma, contenida en la plataforma virtual de la empresa, como servidores, dispositivos de red para almacenamiento de información, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El departamento de informática junto con el responsable de seguridad, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma.

➢ CONTROL ACCESO LOGICO

Los responsables de la administración de la infraestructura tecnológica de INDEA asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por el responsable de seguridad de la información.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el departamento de informática, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada en los procedimientos.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de INDEA, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

➢ GESTION DE CONTRASEÑAS DE USUARIOS

Todos los recursos de información críticos del INDEA tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada empleado requiera para el desarrollo de sus funciones, definidos y aprobados por el departamento de informática y por el responsable de seguridad de la información.

Todo trabajador o tercero que requiera tener acceso a los sistemas de información de INDEA debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso de un usuario (ID) y contraseña (password) asignado por la organización. El trabajador debe ser responsable por el buen uso de las credenciales de acceso asignadas.