



Nombre del instituto: Instituto Tecnológico de Tlalnepantla

Carrera: Ingeniería en tecnologías de la información y comunicación

Materia: Tecnologías de la seguridad en software

Profesor: Hilda Diaz Rincón

Nombre de los alumnos: Diana Godínez Roblero & Zúñiga Morales Noé

Grupo: T-92

Actividad: AVANCES DÍA 27 DE MAYO A10-A12 DEL ISO 27002



Índice

Introducción	6
Selección de departamentos	7
A5 Políticas de seguridad de la información.....	7
5.1 Directrices de gestión de la seguridad de la información.....	7
5.1.1 Políticas para la seguridad de la información.....	7
5.1.2 Revisión de las políticas para la seguridad de la información	7
A6 Organización de la seguridad de la información	8
6.1 Organización interna.....	8
6.1.1 Roles y responsabilidades en seguridad de la información.....	8
6.1.2 Seguridad de tareas.....	8
6.1.3 Contacto con las autoridades.....	8
6.1.4 Contacto con grupos de interés	8
6.1.5 Seguridad de la información en la gestión de proyectos	9
6.2 Los dispositivos móviles y el teletrabajo.....	9
6.2.1 Políticas de dispositivos móviles.....	9
6.2.2 Teletrabajo.....	9
A7. Seguridad relativa a los recursos de la información.....	10
7.1 Antes del empleo	10
7.1.1 Investigación de antecedentes	10
7.1.2 Términos y condiciones del empleo.....	10
7.2 Durante el empleo	10
7.2.1 Responsabilidad de gestión	10
7.2.2 Concienciación, educación y capacitación en seguridad de la información ...	11
A8. Gestión de activos	12
8.1 Responsabilidad sobre los activos	12
8.1.1 Inventario de activos	12
8.1.3 Uso aceptable de los activos.....	12
8.2 Clasificación de la información	12
8.2.1 Clasificación de la información.....	12
8.2.3 Manipulado de la información	13
8.3 Manipulación de los soportes.....	13
8.3.2 Eliminación de soportes	13
A9 Control de acceso	14

9.1 Requisitos de negocio para el control de acceso.....	14
9.1.1 Política de control de acceso	14
9.1.2 Acceso a las redes y a los servicios de red.....	14
9.2 Gestión de acceso de usuarios.....	14
9.2.1 Registro y baja de usuarios.....	14
9.2.4 Gestión de la información secreta de autenticación de los usuarios	15
9.2.5 Revisión de los derechos de acceso de usuario	15
9.3 Responsabilidades del usuario.....	15
9.3.1 Uso de la información secreta de autenticación	15
A10 Criptografía	16
10.1 Controles criptográficos.....	16
10.1.1 Políticas de uso de los controles criptográficos	16
10.1.2 Gestión de claves.....	16
A11 Seguridad física y del entorno	17
11.1 Áreas seguras	17
11.1.1 Perímetro de seguridad física	17
11.1.2 Controles físicos de entrada	17
11.1.3 Seguridad de oficinas, despachos y recursos	17
11.2 Seguridad de los equipos	18
11.2.1 Emplazamiento y protección de equipos.....	18
11.2.2 Instalaciones de suministro	18
11.2.3 Seguridad del cableado.....	18
11.2.4 Mantenimiento de los equipos.....	19
11.2.7 Reutilización o eliminación segura de equipos	19
A12 Seguridad de las operaciones	20
12.1 Procedimientos y responsabilidades operacionales.....	20
12.1.1 Documentación de procedimientos de operación.....	20
12.1.3 Gestión de capacidades	20
12.2 Protección contra el software malicioso (malware)	21
12.2.1 Controles contra el código malicioso	21
12.3 Copias de seguridad	21
12.3.1 Copias de seguridad de la información	21
12.4 Registros y supervisión	22
12.4.1 Registro de eventos	22

12.4.2 Protección de la información del registro	22
A13 Seguridad de las comunicaciones.....	23
13.1 Gestión de la seguridad de redes	23
13.1.1 Controles de red	23
13.1.2 Seguridad de los servicios de red	23
13.2 Intercambio de información	23
13.2.3 Mensajería electrónica.....	23
13.2.4 Acuerdos de confidencialidad o no revelación	24
A14 Adquisición, desarrollo y mantenimiento de los sistemas de información	25
14.1 Requisitos de seguridad en los sistemas de información	25
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información....	25
14.3 Datos de prueba.....	25
14.3.1 Protección de los datos de prueba	25
A15 Relación con proveedores	26
15.1 Seguridad en las relaciones con proveedores	26
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	26
15.2 Gestión de la provisión de servicios del proveedor	26
15.2.1 Control y revisión de la provisión de servicios del proveedor.....	26
A16 Gestión de incidentes de seguridad de la información	27
16.1 Gestión de incidentes de seguridad de la información y mejoras.....	27
16.1.1 Responsabilidades y procedimientos	27
16.1.2 Notificación de los eventos de seguridad de la información.....	27
16.1.3 Notificación de puntos débiles de la seguridad.....	27
16.1.5 Respuesta a incidentes de seguridad de la información	28
16.1.6 Aprendizaje de los incidentes de seguridad de la información	28
16.1.7 Recopilación de evidencias	28
A17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	29
17.1 Continuidad de la seguridad de la información.....	29
17.1.1 Planificación de la continuidad de la seguridad de la información.....	29
17.2 Redundancias.....	29
17.2.1 Disponibilidad de los recursos de tratamiento de la información	29
A18 Cumplimiento.....	30

18.1 Cumplimiento de los requisitos legales y contractuales.....	30
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales ..	30
18.1.2 Derechos de propiedad intelectual (DPI)	30
18.1.3 Protección de los registros de la organización	30
18.1.4 Protección y privacidad de la información de carácter personal.....	31
18.1.5 Regulación de los controles criptográficos	31
18.2 Revisiones de la seguridad de la información.....	31
18.2.1 Revisión independiente de la seguridad de la información.....	31
18.2.2 Cumplimiento de las políticas y normas de seguridad.....	32
18.2.3 Comprobación del cumplimiento técnico	32
Conclusión Noé	33
Conclusión Diana	33
Bibliografía.....	34
Evidencia.....	34
Anexos.....	37
Anexo 1 EJEMPLOS DE CLÁUSULAS QUE SUELEN SER INCLUÍDAS EN UN ACUERDO DE CONFIDENCIALIDAD	37

Introducción

A7. Seguridad relativa a los recursos, A8. Gestión de activos y A9. Control de acceso de la ISO 27002 nos ayudan a implementar sistemas de seguridad de información o mejorar los ya existentes en el laboratorio de cómputo, la zona de cómputo de la biblioteca y el departamento de servicios escolares del Instituto Tecnológico de Tlalnepantla.

Selección de departamentos

Para la actividad 2 se tomará la opción 1 y se seleccionará para aplicar en el laboratorio de cómputo, zona de cómputo de la biblioteca y servicios escolares.

A5 Políticas de seguridad de la información

5.1 Directrices de gestión de la seguridad de la información

Objetivo.

Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes

5.1.1 Políticas para la seguridad de la información

Control.

Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Implementación.

Asignación de responsables y responsabilidades generales y específicas en relación a la seguridad de la información que se maneja, atendiendo las necesidades de los alumnos, docentes o administrativos que soliciten material o información a la que no tienen acceso con regularidad.

Debe contemplarse la seguridad física, ambiental y digital de la información, así como también a las copias de respaldo que se deben tener en caso de algún accidente completamente imprevisto

5.1.2 Revisión de las políticas para la seguridad de la información

Control.

Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Implementación.

En cuanto uno de los servicios sea proporcionado, quien lo haya solicitado pasa a ser el propietario, quien será responsable de todo lo que ocurra con la información, siendo objetivo con la revisión y evaluación de que posee.

A6 Organización de la seguridad de la información

6.1 Organización interna

Objetivo:

Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

6.1.1 Roles y responsabilidades en seguridad de la información

Control:

Todas las responsabilidades en seguridad de la información deberían definirse y asignarse.

Implementación:

Debe asegurarse la protección de todos los activos, por medio de métodos de seguridad específicos para cada uno de ellos, definiendo responsabilidades locales para su protección

6.1.2 Seguridad de tareas

Omitida, el control ya está implementado dentro de los departamentos.

6.1.3 Contacto con las autoridades

Control:

Deberían mantenerse los contactos apropiados con las autoridades pertinentes.

Implementación:

Contacto con el personal de seguridad de la institución en caso de que algún activo se reporte como extraviado o no entregado, haciendo cumplir con el reglamento escolar de que todo alumno que se vea comprometido con material de la institución será sancionado.

6.1.4 Contacto con grupos de interés

Control:

Debería mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

Implementación:

Los grupos de interés general relevancia para dos de los departamentos seleccionados, laboratorio de compito y biblioteca, ya que si hay una correcta supervisión de los activos y se es responsable de lo que ocurre dentro de ellos, pueden ser acreedores a mejorar sus respectivas instalaciones, incluyendo, mobiliario, equipos de computo y material de lectura.

6.1.5 Seguridad de la información en la gestión de proyectos

Control:

La seguridad de la información debería tratarse dentro de la gestión de proyectos, independientes de la naturaleza del proyecto.

Implementación:

Los riesgos de seguridad serán identificados previamente a que ocurran. es decir, se revisarán los historiales de los solicitantes, para establecer la responsabilidad y seguridad de que lo que ha solicitado será bien cuidado y devuelto de forma apropiada.

6.2 Los dispositivos móviles y el teletrabajo

Objetivo:

Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.

6.2.1 Políticas de dispositivos móviles

Omitida. El instituto no cuenta con dispositivos móviles como material institucional.

6.2.2 Teletrabajo

Control:

Se debería implementar una política y unas medidas de seguridad adecuada para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Implementación:

Regulaciones de normas de clases en linea dentro de la institución, dando acceso solo a aplicaciones y paginas autorizadas por la institución, siendo Google, Microsoft Teams, y en algunos casos Zoom, haciendo uso de ellas solo para fines relacionados con el aspecto académico. Dando también autorización de forma independiente a la relacionada con dichas plataformas, a paginas web que ayuden con el cumplimiento de dichas actividades.

A7. Seguridad relativa a los recursos de la información

7.1 Antes del empleo

Objetivo:

Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

7.1.1 Investigación de antecedentes

Control:

Comprobación de los antecedentes de los candidatos al puesto de trabajo debe de llevarse de acuerdo a las leyes, normativas y códigos éticos que sean de aplicación, debiendo ser proporcionales a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos

Implementación:

Los candidatos deberán probar que la información presentada en su currículum vitae es verídica y cumplen con las competencias necesarias para desarrollar roles en seguridad, ya que la información que manejan los departamentos seleccionados es de estado crítico.

7.1.2 Términos y condiciones del empleo

Control:

Como parte de las actividades contractuales, los empleados y contratistas deben establecer términos y condiciones en contrato de trabajo en que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

Implementación:

Todo el personal que accedan a información sensible deberá firmar un compromiso de confidencialidad y no revelación previa a que les sea otorgado el acceso a los recursos. Los empleados tendrán la responsabilidad de clasificar y gestionar la información de los departamentos en los que se desempeñen.

7.2 Durante el empleo

Objetivo:

Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad informática

7.2.1 Responsabilidad de gestión

Control:

La dirección exige a los empleados, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

Implementación:

El personal será debidamente informado de sus responsabilidades a seguridad de la información previamente a brindarles el acceso a información sensible, demostrando

apoyo a políticas y controles de seguridad de la información dentro de los departamentos.

7.2.2 Concienciación, educación y capacitación en seguridad de la información

Control:

Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

Implementación:

Programas de concienciación diseñados de acuerdo a las funciones del personal en sus respectivas áreas, debiendo incluirse actividades que brinden información respecto a nuevas políticas y procedimientos de seguridad relevantes de forma regular.

A8. Gestión de activos

8.1 Responsabilidad sobre los activos

Objetivo:

Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

8.1.1 Inventario de activos

Control:

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

Implementación:

Se enlistarán todos los inventarios tomando en cuenta cuales de estos manejan información sensible para el funcionamiento del área, así como activos que involucren información sobre estudiantes y personal de la institución.

8.1.3 Uso aceptable de los activos

Control:

Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

Implementación:

Establecer un reglamento de uso para el uso de los activos tomando en cuenta la integridad de los mismas y las tareas designadas a cada área en función del horario y el uso de los activos estará restringido por control parental.

8.2 Clasificación de la información

Objetivo:

Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control:

La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

Implementación:

La información solo será manejada por personal autorizado y esta se encontrará protegida por contraseña y será clasificada de acuerdo a que área pertenece.

8.2.3 Manipulado de la información

Control:

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Implementación:

De acuerdo a la clasificación hecha en el punto 8.2.1 se establece quien tiene acceso a la información de acuerdo a cada área.

8.3 Manipulación de los soportes

Objetivo:

Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

8.3.2 Eliminación de soportes

Control:

Los soportes deberían eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

Implementación:

Eliminar los soportes escritos por medio de la destrucción de los mismos de tal forma que la información de estos sea inteligible, además de mezclarse y separarse en contenedores diferentes.

A9 Control de acceso

9.1 Requisitos de negocio para el control de acceso

Objetivo:

Limitar el acceso a los recursos de tratamiento de información y a la información

9.1.1 Política de control de acceso

Control:

Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

Implementación:

El personal tendrá acceso solo a la información que le corresponde, acorde a su puesto y departamento. Solo podrán acceder a información de otros departamentos con permisos extendidos por los encargados de estos.

9.1.2 Acceso a las redes y a los servicios de red

Control:

Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados

Implementación:

El personal tendrá acceso solo a las redes de la escuela, ya que son las más seguras, cada uno de los equipos contara con procedimientos de autorización que otorguen el permiso de conexión a red, de igual forma los servicios serán monitoreados para que se tenga un mejor desempeño.

9.2 Gestión de acceso de usuarios

Objetivo:

Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

9.2.1 Registro y baja de usuarios

Control:

Deberán implementarse procedimientos formales de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso

Implementación:

Identificación de usuarios por medio de identificadores ID, cada uno deberá hacerse responsable de las actividades que se realicen bajo el registro de su ID, para todo personal que deje el departamento o la organización, su ID será dado de baja de forma inmediata

9.2.4 Gestión de la información secreta de autenticación de los usuarios

Control:

La asignación de la información secreta de autenticación debería ser controlada a través de un proceso formal de gestión.

Implementación:

Todos los usuarios que hagan uso de la información de los departamentos seleccionados, deberán acordar mantener confidencialidad de la información, apoyando con su autenticación personal (credencial estudiantil o de docencia), al término del uso de la información seleccionada o deberán confirmar la recepción de esta

9.2.5 Revisión de los derechos de acceso de usuario

Control:

Los propietarios de los derechos de acceso deberían revisar los derechos de acceso de usuario a intervalos regulares

Implementación:

Revisiones regulares de los derechos de acceso del personal, siendo reasignados cuando este cambie de departamento o área, los derechos de acceso privilegiados también serán revisados frecuentemente.

9.3 Responsabilidades del usuario

Objetivo:

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

9.3.1 Uso de la información secreta de autenticación

Control:

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

Implementación:

Antes de acceder a información se debe de presentar un documento que acredite su persona (credencial escolar de preferencia) y naturaleza de lo que realizara (por ejemplo, un oficio)

A10 Criptografía

10.1 Controles criptográficos

Objetivo.

Garantizar un uso adecuado y eficaz de la criptografía para poder proteger la confidencialidad, autenticidad y/o integridad de la información

10.1.1 Políticas de uso de los controles criptográficos

Control.

Se deberá desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información

Implementación.

Solicitud de contraseñas o códigos de verificación para que toda información solicitada, libro prestado o maquina utilizada sea registrada en un historial de alumno o docente. Dicho historial registrara si el usuario hizo uso correcto de lo solicitado y no infringió ninguna regla impuesta por cada uno de los departamentos.

10.1.2 Gestión de claves

Control.

Se deberá desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida

Implementación.

Solicitud de contraseñas o códigos de verificación para que toda información solicitada, libro prestado o maquina utilizada sea registrada en un historial de alumno o docente, cifrando toda la información y siendo solo visible para los encargados de departamento

A11 Seguridad física y del entorno

11.1 Áreas seguras

Objetivo.

Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

11.1.1 Perímetro de seguridad física

Control.

Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.

Implementación.

Poner una banda delimitadora para que solo personal autorizado tenga acceso a determinadas zonas.

11.1.2 Controles físicos de entrada

Control.

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

Implementación.

Restringir la entrada a las áreas sensibles por medio de controles magnéticos como cerraduras con tarjetas de acceso.

11.1.3 Seguridad de oficinas, despachos y recursos

Control

Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.

Implementación.

Contratar personal de seguridad.

11.2 Seguridad de los equipos

Objetivo.

Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

11.2.1 Emplazamiento y protección de equipos

Control.

Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.

Implementación.

Los equipos deberán ser ubicados alejados de las ventanas.

Las zonas donde está ubicado el equipo debe de ser impermeabilizada.

11.2.2 Instalaciones de suministro

Control.

Los equipos deberían estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

Implementación.

Se implementarán Centros de Carga para proteger los equipos.

Se implementará una fuente de energía (generador eléctrico) para que se mantenga el correcto funcionamiento de los equipos.

11.2.3 Seguridad del cableado

Control.

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

Implementación.

Esconder los conductores en canaletas.

El cable para la instalación eléctrica exterior tiene que ser unipolar o multipolar, hecho de cobre y con tensión de 0,6/1kV y este tiene que estar enterrado.

11.2.4 Mantenimiento de los equipos

Control

Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

Implementación.

Contratar personal destinado al mantenimiento de los equipos.

11.2.7 Reutilización o eliminación segura de equipos

Control.

Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

Implementación.

Realizar el formateo de los equipos y reinstalación de SO.

Reemplazar elementos dañados del equipo si es que lo requiere.

A12 Seguridad de las operaciones

12.1 Procedimientos y responsabilidades operacionales

Objetivo.

Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

12.1.1 Documentación de procedimientos de operación.

Control.

Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

Implementación.

Se deberá de realizar un informe por cada procedimiento de operación que se haga y este deberá de ser lo más detallado posible.

Se creará un apartado en la biblioteca con los informes de procedimientos de operación.

12.1.3 Gestión de capacidades

Control.

Se debería supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

Implementación.

Se deben de analizar todos los equipos y generar documentos donde se especifiquen las capacidades máximas de los equipos para poder sacar su máximo potencial de los equipos.

12.2 Protección contra el software malicioso (malware)

Objetivo.

Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.

12.2.1 Controles contra el código malicioso

Control.

Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

Implementación.

Contratar Fortinet.

Para las páginas web: Usar declaraciones prediseñadas, consultas parametrizadas o procedimientos almacenados para garantizar que los elementos SQL en los campos de entrada del usuario nunca se traten como consultas genuinas.

12.3 Copias de seguridad

Objetivo.

Evitar la pérdida de datos.

12.3.1 Copias de seguridad de la información

Control.

Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

Implementación.

Se hará uso de servicios en la nube para generar copias de seguridad de forma periódica o cuando eventos importantes sucedan.

12.4 Registros y supervisión

Objetivo.

Registrar eventos y generar evidencias.

12.4.1 Registro de eventos

Control.

Se deberían registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Implementación.

Registrar semanalmente todos los eventos de las áreas por medio de reportes y en caso de ser un suceso relevante pase, se registrará a su finalización.

12.4.2 Protección de la información del registro

Control.

Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.

Implementación.

Por medio del punto A11 se protegerá la integridad física de la información, así como su resguardo de accesos no autorizados.

A13 Seguridad de las comunicaciones

13.1 Gestión de la seguridad de redes

Objetivo.

Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

13.1.1 Controles de red

Control.

Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

Implementación.

Asignar protocolos de seguridad

Asignar un administrador de red

13.1.2 Seguridad de los servicios de red

Control.

Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

Implementación.

Contratación de Fortinet al igual que en el punto 12.2.1

13.2 Intercambio de información

Objetivo.

Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.

13.2.3 Mensajería electrónica

Control.

La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.

Implementación.

Dar curso de capacitación sobre seguridad en los E-Mails al personal y alumnado.

13.2.4 Acuerdos de confidencialidad o no revelación

Control.

Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.

Implementación.

Implementar el contenido del anexo 1.

A14 Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1 Requisitos de seguridad en los sistemas de información

Objetivo.

Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información

Control.

Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Implementación.

Realizar un análisis de los equipos e implementar una simulación de ataque para determinar las vulnerabilidades de los sistemas para redactar un documento con los resultados de estas.

14.3 Datos de prueba

14.3.1 Protección de los datos de prueba

Control.

Los datos de prueba se deberían seleccionar con cuidado y deberían ser protegidos y controlados.

Implementación.

Se debería evitar el uso de datos reales de operación que contengan datos personales o cualquier otra información confidencial para las pruebas. Si se utiliza la información de datos personales o información confidencial para las pruebas, todos los detalles y contenidos sensibles deberían protegerse mediante su retirada o su modificación.

A15 Relación con proveedores

15.1 Seguridad en las relaciones con proveedores

Objetivo.

Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 Política de seguridad de la información en las relaciones con los proveedores

Control.

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deberían acordarse con el proveedor y quedar documentados.

Implementación.

La organización debería identificar y encargar los controles de seguridad de información para abordar específicamente el acceso de los proveedores a la información de la organización como norma obligatoria para tener acceso al plantel.

15.2 Gestión de la provisión de servicios del proveedor

Objetivo.

Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

15.2.1 Control y revisión de la provisión de servicios del proveedor

Control.

Las organizaciones deberían controlar, revisar y auditar regularmente la provisión de servicios del proveedor.

Implementación.

La supervisión y la revisión de los servicios de proveedores deberían asegurar que los términos y las condiciones de seguridad de la información de los acuerdos se están cumpliendo y que los incidentes y problemas de seguridad de la información se gestionan adecuadamente.

A16 Gestión de incidentes de seguridad de la información

16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo.

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Control.

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

Implementación.

Las responsabilidades y procedimientos deberán ser especificados de acuerdo a las directrices de cada área de forma independiente, aun cuando realizan actividades diferentes.

16.1.2 Notificación de los eventos de seguridad de la información

Control.

Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.

Implementación.

Dentro de todos los contratos y procedimientos debe de haber un apartado que especifique que todos los trabajadores, contratistas y terceros deberían conocer su responsabilidad de comunicar cualquier evento de seguridad de la información lo antes posible.

Deberían conocer el procedimiento de comunicación de eventos de seguridad de la información y el punto de contacto.

16.1.3 Notificación de puntos débiles de la seguridad

Control.

Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

Implementación.

Dentro de todos los contratos y procedimientos debe de haber un apartado que especifique que todos los trabajadores, contratistas y terceros deberían conocer los puntos débiles de la seguridad si es que los detectan y de ser posible, sugerir una solución por escrito.

16.1.5 Respuesta a incidentes de seguridad de la información

Control.

Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.

Implementación.

Establecer protocolos de respuesta dependiendo de que evento sucedió y en qué área.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

Control.

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

Implementación.

Se deberán de utilizar los informes creados en la implementación del punto 16.1.5 para actualizar las medidas de seguridad mencionadas en puntos anteriores.

16.1.7 Recopilación de evidencias

Control.

La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.

Implementación.

Hacer informes por cada incidente si es que sucede y se debe de documentar que sucedió, como sucedió, el motivo y como se solucionó.

A17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

17.1 Continuidad de la seguridad de la información

Objetivo.

La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información

Control.

La organización debería determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Implementación.

la continuidad de la seguridad de la información queda dentro del proceso de continuidad del negocio.

17.2 Redundancias

Objetivo.

Asegurar la disponibilidad de los recursos de tratamiento de la información.

17.2.1 Disponibilidad de los recursos de tratamiento de la información

Control.

Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

Implementación.

Se deberán de identificar los requisitos de disponibilidad para los sistemas de información. Cuando la disponibilidad no pueda garantizarse usando la arquitectura de sistemas existentes, deberían considerarse componentes o arquitecturas redundantes.

A18 Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales

Objetivo.

Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control.

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.

Implementación.

Contratar un servicio de auditoría jurídica.

Identificar toda la legislación aplicable para cumplir con los requisitos de cada área.

18.1.2 Derechos de propiedad intelectual (DPI)

Control.

Deberían implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Implementación.

Crear y aplicar una política para el cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos software y de la información.

Mantener pruebas y evidencias de la propiedad de las licencias.

18.1.3 Protección de los registros de la organización

Control.

Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

Implementación.

Se deberían establecerse procedimientos que aseguren el acceso a los datos durante el periodo de retención con el fin de proteger contra la pérdida causada por futuros cambios de la tecnología.

18.1.4 Protección y privacidad de la información de carácter personal

Control.

Debería garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Implementación.

Desarrollar e implantar una política de privacidad y protección de la información de carácter personal con fundamento en LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS.

18.1.5 Regulación de los controles criptográficos

Control.

Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

Implementación.

Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.

18.2 Revisiones de la seguridad de la información

Objetivo.

Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

18.2.1 Revisión independiente de la seguridad de la información

Control.

El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

Implementación.

Se contratará un servicio de auditoria que revise los requisitos de seguridad de la información definidos en las políticas, normas y otra reglamentación a cumplir.

18.2.2 Cumplimiento de las políticas y normas de seguridad

Control.

Los directivos deberían asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

Implementación.

Si se identifica algún incumplimiento, los directivos o responsables deberían de identificar las causas del incumplimiento, evaluar las acciones necesarias para el cumplimiento y hacer un informe donde se detalle todo lo anterior para posteriormente entregar a los directivos y ejecutén las acciones correctivas necesarias.

18.2.3 Comprobación del cumplimiento técnico

Control.

Debería comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Implementación.

El cumplimiento técnico debería revisarse preferiblemente con la ayuda de herramientas automáticas que generen informes técnicos que posteriormente interprete un especialista técnico ya sea externo o interno.

Toda revisión de cumplimiento técnico debería tan solo realizarse por personal competente y autorizado o bajo la supervisión de dichas personas.

Conclusión Noé

En conclusión, el uso de las normas ISO 27001 y 27002, no es algo rígido a seguir si no que es más una recomendación, pues es flexible para usar por separado, es decir se pueden utilizar apartados sin necesidad de ponerla completamente

Conclusión Diana

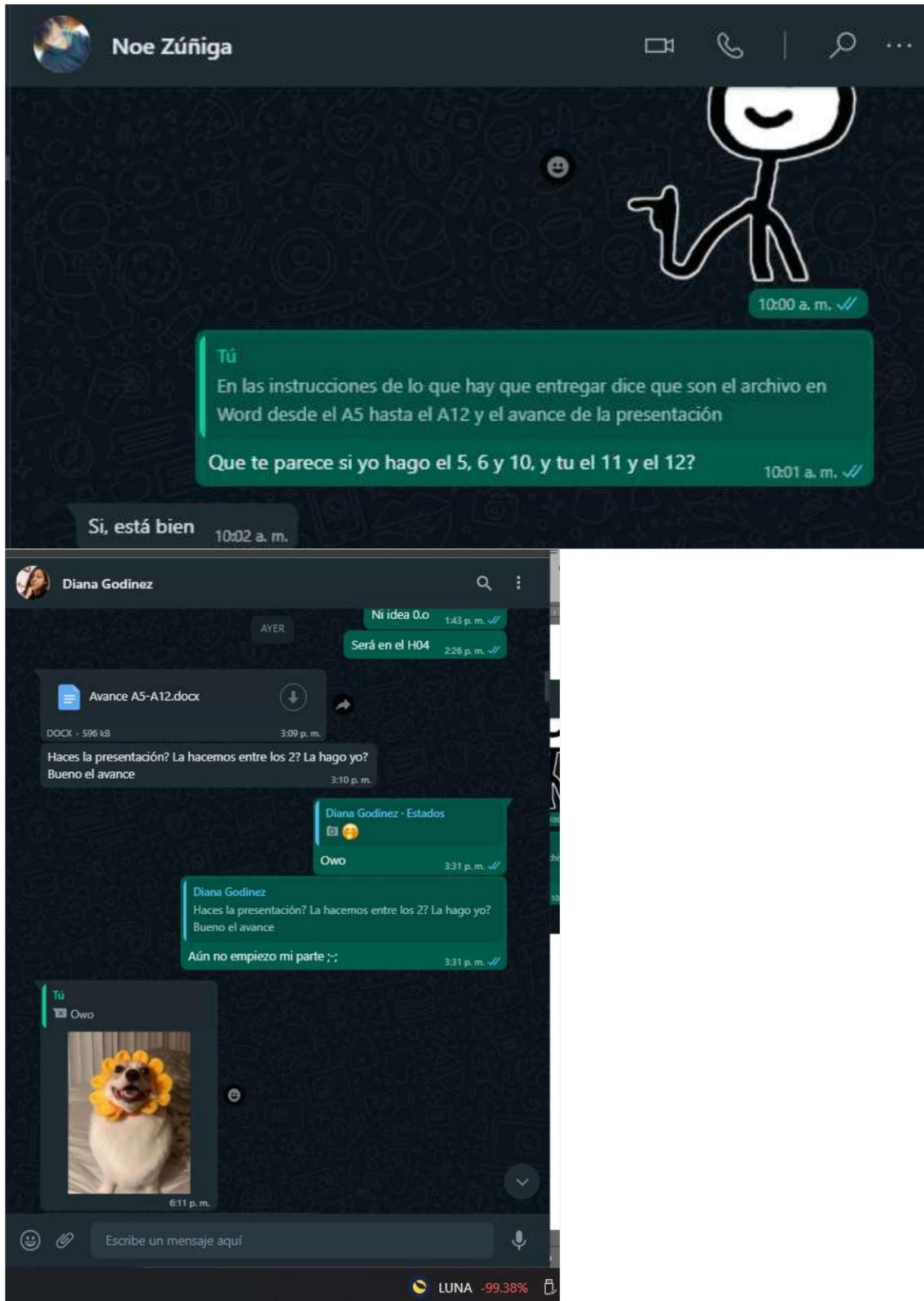
El conocimiento de las Normas ISO 27001 e ISO 27002 nos ayudan a entender como aplicarlas y desarrollarlas adecuadamente para poder obtener una certificación. Para el trabajo que empezamos a desarrollar nos ayudan a pensar que en todas las implantaciones que hagamos debemos incluirlas, es decir, debemos pensar que la actividad debe tener una calidad que se acerque a la autorización de una fase inicial de auditoría

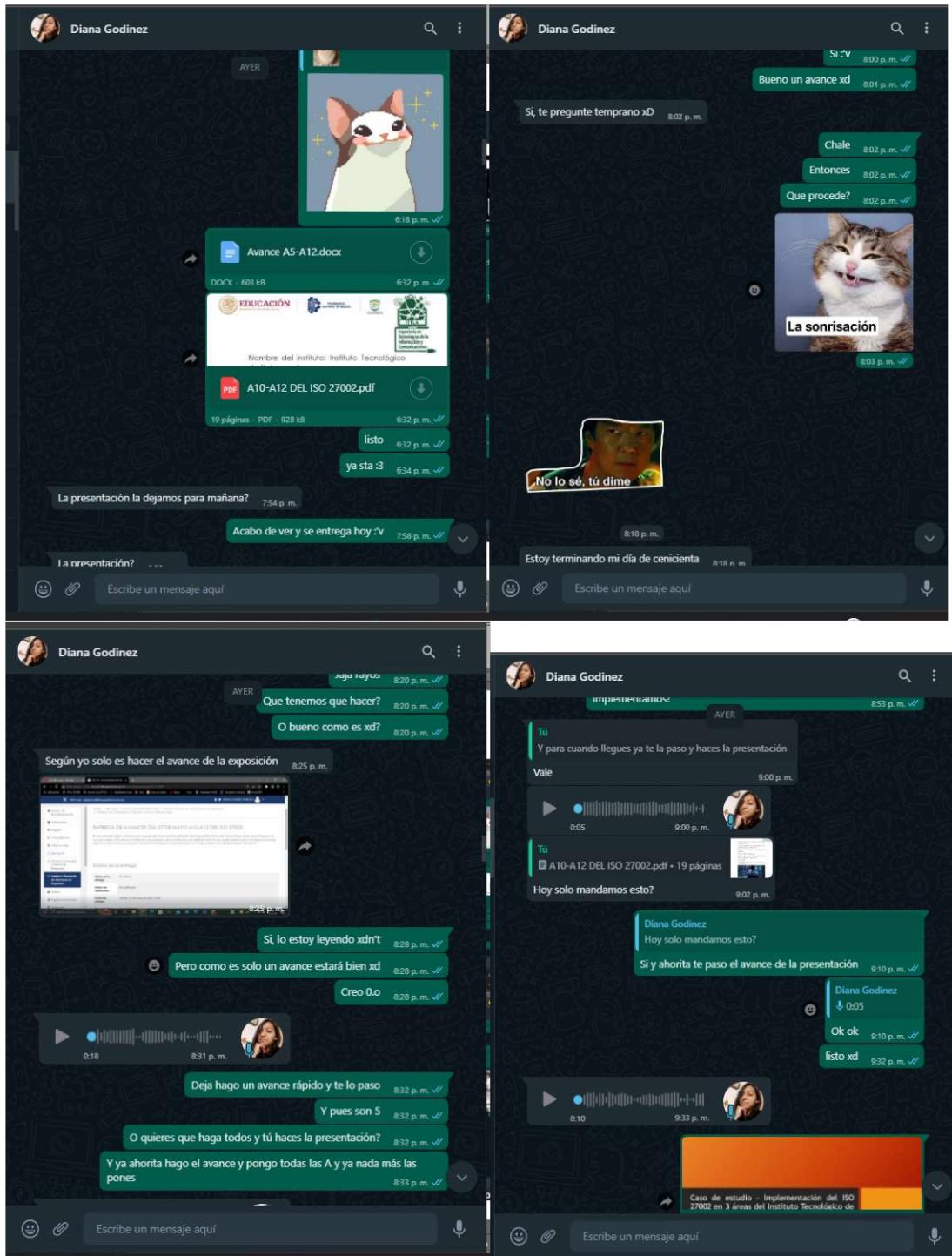
Bibliografía

Industria Conectada 4.0 - Normas UNE-EN ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para la seguridad de la información. (2022). Retrieved May 25, 2022, from Industriaconectada40.gob.es website:
<https://www.industriaconectada40.gob.es/difusion/noticias/Paginas/Normas-UNE-EN-ISOIEC-27001-UNE-EN-ISOIEC-27002-seguridad-de-informaci%C3%B3n.aspx>

Evidencia







Anexos

Anexo 1 EJEMPLOS DE CLÁUSULAS QUE SUELEN SER INCLUÍDAS EN UN ACUERDO DE CONFIDENCIALIDAD

A continuación, se exponen ejemplos de diversas cláusulas que se suelen incluir en un acuerdo de confidencialidad. El contenido definitivo de un acuerdo de este tipo así como la redacción de sus cláusulas, dependerá del resultado de la negociación sostenida entre las partes contratantes.

Ejemplo de cláusula en que se describe la información confidencial:

"Las partes exponen que las negociaciones llevadas a cabo (o el proyecto a desarrollar en conjunto) entre el titular de la información descrita a continuación, en adelante el Divulgador, y el receptor de la misma, en adelante el Receptor, han involucrado o involucrarán divulgación escrita o verbal y comunicación al Receptor por parte del Divulgador o por miembros de su equipo de trabajo, de documentos propios o controlados por alguno de los mencionados anteriormente, la que puede incluir, pero no se limita a información financiera, planes de negocios, información personal, dibujos, ejemplos y prototipos de artefactos, demostraciones, secretos comerciales, información técnica, sistemas de computación y software, resultados de investigaciones, listas de clientes y otros datos en forma oral o escrita, relacionada con la tecnología, ya sea que dicha comunicación se produzca verbalmente, visualmente, o mediante demostraciones o cualquier otro medio, tanto en forma de dibujos, modelos, documentos impresos, y/o formato de archivos electrónicos o de cualquier otra manera, en adelante la Información"

Ejemplo de cláusula que describe el objeto de un acuerdo de confidencialidad.

"El receptor desea recibir o utilizar la información confidencial con el propósito de poder evaluar la suscripción de un futuro acuerdo de _____, entre ambos/ desarrollar un proyecto de _____ en conjunto, para lo cual otorgan el acuerdo del que da cuenta este instrumento. Para estos efectos, cada parte indicará a la otra parte, por escrito, quienes serán las personas (máximo_) que dentro de su organización estarán autorizadas para entregar o recibir la Información según el caso."

Ejemplo de cláusula sobre la propiedad de la información confidencial.

"La información confidencial, y todos los derechos a la misma que han sido o serán divulgados al Receptor, permanecerán como propiedad del Divulgador. El Receptor no obtendrá derecho alguno, de ningún tipo, sobre la información, ni tampoco ningún derecho de utilizarla, excepto para el objeto del presente acuerdo. La divulgación de la Información confidencial no implica el licenciamiento de derecho de patentes o derecho de autor o ningún otro derecho por parte del Divulgador, que no sean los establecidos aquí."

Ejemplo de cláusula que establece obligaciones para el receptor de la información confidencial.

“Además de las obligaciones que emanen de la naturaleza del acuerdo del que da cuenta el presente instrumento el receptor de la información confidencialidad estará obligado a:

Mantener la información confidencial en estricta reserva y no revelar ningún dato de la información a ninguna otra parte, relacionada o no, sin el consentimiento previo escrito del divulgador.

Instruir al personal que estará encargado de recibir la información confidencial, debiendo suscribir el correspondiente acuerdo de confidencialidad si fuere necesario, de su obligación de recibir, tratar y usar la información confidencial que reciban como confidencial y destinada únicamente al propósito objeto del acuerdo, en los mismos términos en que se establece en el presente instrumento.

Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización.

Tratar confidencialmente toda la información recibida directa o indirectamente del divulgador, y no utilizar ningún dato de esa información de ninguna manera distinta al propósito del presente acuerdo.

No manejar, usar, explotar, o divulgar la información confidencial a ninguna persona o entidad por ningún motivo en contravención a lo dispuesto en este instrumento, salvo que sea expresamente autorizado por escrito a hacerlo por el divulgador.”

Ejemplo de cláusula sobre obligación de indemnizar en caso de infracción.

“La divulgación o el uso de la Información por el Receptor en infracción de este acuerdo será considerado causal de indemnización de perjuicios.”

Ejemplo de cláusula sobre la reproducción de la información confidencial.

“La información confidencial no podrá ser reproducida por ningún medio ni en ningún formato por el Receptor sin expresa autorización previa escrita del Divulgador, excepto por aquellas copias que el Receptor pueda necesitar para hacer operativo este acuerdo.

En caso que el Receptor fuere autorizado por el Divulgador a reproducir total o parcialmente la información confidencial, todas las reproducciones, sean totales o parciales y cualquiera sea el formato en que se registren, deberán hacer expresa mención a la propiedad intelectual del Divulgador sobre la información contenida en ellas, contando con anuncios de confidencialidad y manteniendo las leyendas que contenga la Información original, salvo que el Divulgador disponga otra cosa por escrito”.

Ejemplo de cláusula de excepción a la obligación de confidencialidad.

“Las obligaciones previstas en el presente instrumento no se aplicarán en los siguientes casos:

i. Si se trata de información que sea de dominio público, o en lo sucesivo pase a ser de dominio público, por medios diferentes de una actividad no autorizada o una omisión del receptor; o se trate de información que obre en poder del receptor y no esté sujeta a obligaciones de secreto y no haya sido obtenida del divulgador; o se trate de información que deba divulgarse en virtud de la legislación vigente o por disposición de la autoridad o tribunales de justicia.

ii. Si la Información o cualquier parte de ella es legalmente obtenida por el Receptor de una tercera parte o partes sin infracción de este acuerdo por el Receptor, demostrando que la tercera parte es una fuente legal de Información.

iii. Si la Información o cualquier parte de ella fue conocida por el Receptor antes de su divulgación por el Divulgador siempre que el Receptor sea capaz de acreditar dicho conocimiento.

El Receptor reconoce que no se incluirá entre las excepciones mencionadas ninguna combinación de características por el mero hecho de que cada una de ellas sea de dominio público u obren en poder del Receptor. El Receptor será responsable de demostrar sus derechos con respecto a cualquier excepción prevista en la presente cláusula.”

Ejemplo de cláusula sobre devolución de información.

“En cualquier momento, ante solicitud escrita del Divulgador, el Receptor devolverá a éste toda o parte de la Información según lo requiera el Divulgador así como las copias que se encuentren en su poder cualquiera sea su formato. A requerimiento del Divulgador el Receptor deberá destruir la Información y proporcionar prueba de su destrucción al Divulgador”.

Ejemplo de cláusula de limitación de responsabilidad del Divulgador.

“Este acuerdo no constituye garantía para el Receptor por parte del Divulgador respecto a la posible infracción de patentes u otros derechos de terceras partes relacionados con la Información. El Divulgador no será responsable, por el plazo de duración de la divulgación, por los errores u omisiones en la Información y por el uso y los resultados del uso de esta Información.

El Divulgador no será responsable en modo alguno de ninguna pérdida de ningún tipo, incluidos sin excepción, los daños y perjuicios, costos intereses, pérdidas de beneficios, ni de otras pérdidas o perjuicios similares derivados de cualquier error, inexactitud, omisión o cualquier otro defecto en la información.”

Otras estipulaciones que pueden ser incorporadas en un acuerdo de confidencialidad, pueden ser revisadas en el siguiente documento (Cláusulas generales distintos contratos de transferencia de tecnología).