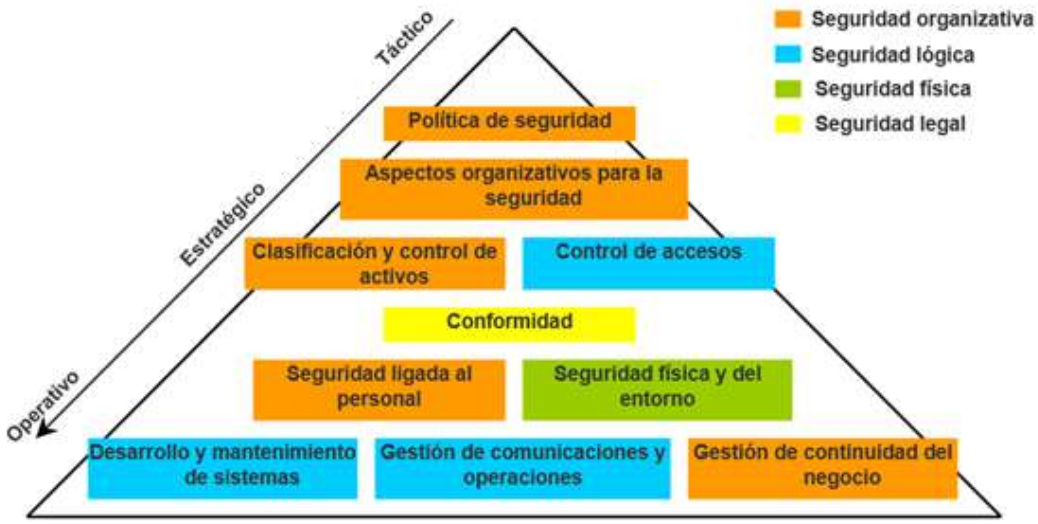
UNIVERSIDAD DE BURGOS

ISO 17799



Eduardo Mora González

Contenido

1. INTRODUCCIÓN

La información es un activo que es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente y más actualmente en un ambiente comercial cada vez más interconectado, ya que la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Por eso la norma ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. La seguridad de la información se define como la preservación de:

- **Confidencialidad.** Garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.
- **Disponibilidad.** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- **Integridad.** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

Por eso objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

2. NORMA ISO 17799

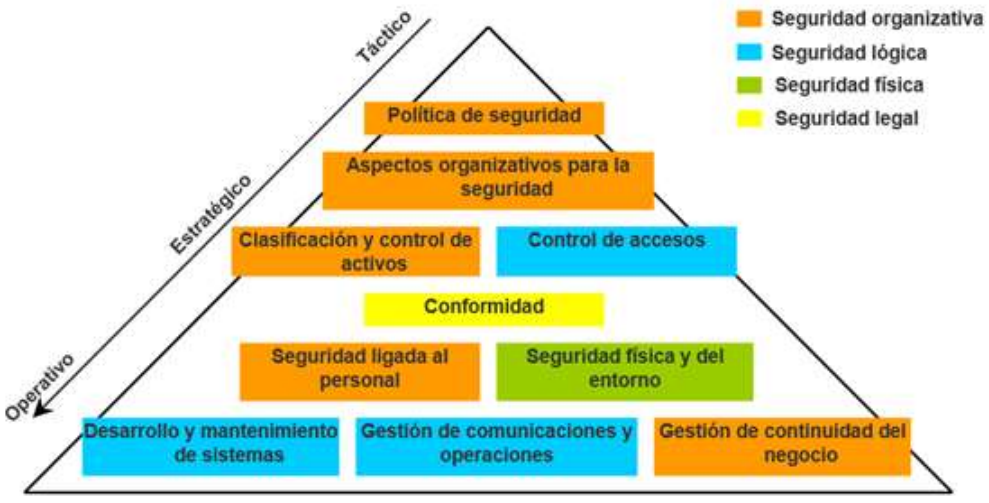
La norma contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cada cláusula contiene un número de categorías de seguridad principales, las cláusulas son:

1. Política de Seguridad
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
9. Gestión de Incidentes de Seguridad de la Información
10. Gestión de la Continuidad Comercial
11. Conformidad

Cada categoría de seguridad contiene un objetivo de control que establece lo que se debiera lograr; y uno o más controles que se pueden aplicar para lograr el objetivo de control.

La norma se puede estructurar de la siguiente forma [R1]:



2.1. EVALUACIÓN Y TRATAMIENTO DEL RIESGO

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización.

Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos.

En las evaluaciones se deberían incluir el enfoque sistemático de calcular la magnitud de los riesgos y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos.

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo. Por esta razón, las evaluaciones se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

Las evaluaciones deberían tener un criterio de aceptación del riesgo, y si este es aceptado, deben definir la forma de tratar el riesgo.

Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicar los controles apropiados para reducir los riesgos.
b) Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización.
c) Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.
d) Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo.

Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales.
b) Objetivos organizacionales.
c) Requerimientos y restricciones operacionales.
d) Costo de implementación y operación en relación con los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización.
e) La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

3. CLÁUSULAS DE CONTROL DE LA ISO-17799

A continuación, se verán todas las 4 primeras cláusulas de una forma detallada.

3.1. POLÍTICA DE SEGURIDAD

El objetivo principal de esta clausura es proporcionar a la gerencia unas directrices el tratamiento de la seguridad de la información en concordancia con los requerimientos comerciales, leyes y regulaciones relevantes.

La política de seguridad de una organización debe estar definido por la alta dirección. Una vez desarrollada debe ser aprobada y publicada para que le llegue a todo el personal implicado.

El documento de la política de seguridad deberá contener puntos relacionados con:

- La definición de seguridad de la información, sus objetivos y alcance.
- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.

- Una explicación resumida de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización.
- Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información.

Como bien se ha dicho antes, una vez desarrollada la política de seguridad, se debe revisada. La revisión de la política de seguridad debiera tomar en cuenta los resultados de las revisiones de la gerencia y debieran existir procedimientos de revisión gerencial, incluyendo un cronograma o el período de la revisión.

3.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gerencia debería realizar y aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización interna y externa.

3.2.1. ORGANIZACIÓN INTERNA

Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización y si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Estas fuentes deben mantener contacto con los especialistas o grupos de seguridad externos para mantenerse actualizado.

La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

También, la gerencia debiera identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización.

Por otro lado, las actividades de la seguridad de la información debieran ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes. Esta coordinación debiera entre otras cosas:

- Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información en el caso de que existan no-conformidades se deben identificar cómo manejarlas.
- Aprobar las metodologías y procesos para la seguridad de la información.
- Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas realizando una evaluación continua.
- Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.

Si la organización no utiliza grupos interfuncionales separados, las acciones arriba descritas debieran ser realizadas por otro organismo gerencial adecuado o un gerente individual.

El organismo gerencial junto con todas las responsabilidades de la seguridad de la información debiese estar claramente definidas y deben ser los encargados de la autorización y desarrollo de nuevas facilidades de procesamiento de información, tanto como debiera ser definido como implementado. La guía de implementación de este proceso de autorización en la siguiente:

- Las nuevas facilidades debieran tener apropiadas autorizaciones gerenciales para su autorización, autorizando su uso apropiado.
- Donde sea necesario, el hardware y el software debiera de ser chequeado para asegurar que son compatibles con otros componentes del sistema.
- El uso de facilidades para el procesamiento de información, bien sean personales o privadas.

Por otro lado, se debieran identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la organización para proteger la información.

Finalmente, se debiera revisar el enfoque de la organización para manejar la seguridad de la información y su implementación de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.

3.2.2. GRUPOS O PERSONAS EXTERNAS

La seguridad de la información y los medios de procesamiento de la información de la organización no debieran ser reducidos por la introducción de productos y servicios de grupos externos.

Se debiera controlar cualquier acceso a los medios de procesamiento de información de la organización y el procesamiento y comunicación de la información realizado por grupos externos.

Para controlar esto, se debieran identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se debieran implementar controles apropiados antes de otorgarles acceso.

Y no se debiera otorgar acceso a los grupos externos a la información de la organización hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato definiendo los términos y condiciones para la conexión o acceso y el contrato de trabajo.

Se debieran tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización. Se debieran considerar entre otros los siguientes términos de seguridad antes de proporcionar a los clientes acceso a cualquier activo de la organización:

- Protección de activos, incluyendo información, software, integridad…
- Política de control de acceso.
- Una descripción de cada servicio que debiera estar disponible.
- El nivel objetivo del servicio y los niveles inaceptables del servicio.
- Responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales.

Para los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o medios de procesamiento de información de la compañía, o agregan producto o servicios a los medios de procesamiento de información debieran abarcar todos los requerimientos de seguridad relevantes.

Todos estos acuerdos entre la organización y clientes o terceros pueden variar considerablemente para las diferentes organizaciones y entre los diferentes tipos de clientes o terceras personas.

3.3. GESTIÓN DE ACTIVOS

3.3.1. RESPONSABILIDAD POR LOS ACTIVOS

Los propietarios debieran identificar todos los activos, mediante un inventario de los activos donde se debiera incluir toda la información necesaria para poder recuperarse de un desastre, pero sin duplicar otros inventarios.

También se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados; estos controles deben estar basados en la importancia del activo, su valor comercial y su clasificación de seguridad y se debieran identificar los niveles de protección que se conmensuran con la importancia de los activos.

La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos. El propietario del activo debiera ser responsable de:

- Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente.
- Definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

Finalmente, se debieran identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

3.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

La información debiera ser clasificada (en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización) para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

Los lineamientos de clasificación debieran incluir protocolos para la clasificación inicial y la reclasificación a lo largo del tiempo; en concordancia con alguna política predeterminada de control de acceso.

Y por lo mencionado en el punto anterior, debiera ser responsabilidad del propietario del activo definir la clasificación de un activo, revisarla periódicamente y asegurarse que se mantenga actualizada y en el nivel apropiado.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial por lo que se debiera utilizar un esquema de clasificación de información (en concordancia con el esquema de clasificación adoptado por la organización) para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

3.4. SEGURIDAD DE RECURSOS HUMANOS

3.4.1. ANTES DEL EMPLEO

Las responsabilidades de seguridad debieran ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo, para ello se debieran definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

Los antecedentes de todos los candidatos al empleo, contratistas y terceros debieran ser adecuadamente investigados, especialmente para los trabajos confidenciales. Los chequeos de verificación debieran tomar en cuenta la legislación relevante con relación a la privacidad de la data personal y/o empleo; y cuando sea permitido, debiera incluir lo siguiente:

- Disponibilidad de referencias de carácter satisfactorias.
- Un chequeo del curriculum vitae del postulante (buscando integridad y exactitud).
- Confirmación de las calificaciones académicas y profesionales mencionadas.
- Chequeo de identidad independiente (pasaporte o documento similar);
- Chequeos más detallados, como chequeos de crédito o chequeos de récords criminales.

Cuando un puesto de trabajo sea un nombramiento inicial o un ascenso, involucra que la persona tenga acceso a los medios de procesamiento de información, y en particular si las personas manejan información confidencial la organización también debiera considerar chequeos más detallados.

Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información debieran firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad el cual debiera establecer sus responsabilidades y las de la organización para la seguridad de la información.

La organización debiera asegurarse que los usuarios empleados, contratistas y terceras personas acepten los términos y condiciones concernientes a la seguridad de la información apropiada según la naturaleza y extensión del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información.

3.4.2. DURANTE EL EMPLEO

Se debieran definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la organización. La gerencia debiera requerir a los usuarios empleados,

contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.

Si los usuarios empleados, contratistas y terceras personas no son conscientes de sus responsabilidades de seguridad, ellos pueden causar un daño considerable a la organización.

Se debiera proporcionar a todos los usuarios empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad.

Se debiera establecer un proceso disciplinario normal para manejar las fallas en la seguridad. El proceso disciplinario debiera proporcionar una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio.

3.4.3. TERMINACIÓN O CAMBIO DE EMPLEO

Se debieran establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

Las responsabilidades y deberes aún válidos después de la terminación del empleo debieran estar contenidos en los contratos del empleado, contratista o tercera persona.

Todos los usuarios empleados, contratistas y terceras personas debieran devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo

En los casos donde el usuario empleado, contratista o tercera persona compra el equipo de la organización o utiliza su propio equipo, se debieran seguir procedimientos para asegurar que toda la información relevante sea transferida a la organización y sea adecuadamente borrada del equipo.

Finalmente, los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información debieran ser retirados a la terminación de su empleo, contrato o acuerdo, o debieran ser reajustados de acuerdo con el cambio.

Los derechos de acceso para los activos de información y los medios de procesamiento de información se debieran reducir o retirar antes de la terminación o cambio del empleo, dependiendo de la evaluación de los factores de riesgo como:

- Si la terminación o cambio es iniciado por el usuario empleado, contratista o tercera persona, o por la gerencia y la razón de la terminación.
- Las responsabilidades actuales del usuario empleado, contratista o cualquier otro usuario.
- El valor de los activos actualmente disponibles.

REFERENCIAS

R1:https://www.google.com/url?sa=i&url=http%3A%2F%2Faicnerefer.blogspot.com%F2017%2F11%2Fiso17799introduccionsurgidadela.html&psig=AOvVaw3eu4dAPd9rysbQQRRbaJit&ust=1587198600643000&sourc=images&cd=vfe&ved=0CAIQjRxqFwoTCKjB-teF7-gCFQAAAAAdAAAAABAD