Escuela Superior de Redes RED CEDIA

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

VERSIÓN ORIGINAL:
Flávia Estélia Silva Coelho
Luiz Geraldo Segadas de Araújo
Edson Kowask Bezerra

VERSIÓN ADAPTADA AL ECUADOR
A partir de la versión de
ESR RENATA -Colombia

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Gestión de la seguridad de la información

Versión original:
Flávia Estélia Silva Coelho
Luiz Geraldo Segadas de Araújo
Edson Kowask Bezerra

Versión adaptada al Ecuador
A partir de la versión de
ESR RENATA - Colombia

redCEDIA
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Escuela Superior de Redes RED CEDIA

Red Nacional de Tecnología Avanzada - RENATA

Director Ejecutivo
Lucas Giraldo Rios

Gerente de Comunicaciones
Camilo Jaimes Ocazionez

Gerente Administrativo y Financiero
Jader Alexis Castaño

Gerente de Tecnología e Información
Javier Enrique Lizarazo Rueda

Escola Superior de Redes - RNP Brasil

Título original "Gestão da Segurança da Informação NBR 27001 e 27002"
Versión portuguesa RNP ©

Autores versión portuguesa
Flavia Estélia Silva Coelho
Luis Geraldo Segadas de Araújo
Edson Kowask Bezerra

Universidad Nacional de Colombia Facultad de Ingeniería

Decano
José Ismael Peña Reyes

Vicedecano Académico
Oscar Germán Duarte

Director Instituto de Extensión e Investigación
Carlos Cortés

Coordinadora Académica
Jenny Marcela Sánchez-Torres

Autor versión adaptada y ampliada
Hernando Peña Villamil

Traductor
Oscar Edwin Piamba Tulcán

Profesionales de apoyo
Ana Carolina Gómez Parra

Diseño y diagramación
Andrés Camilo Gantiva Rueda

ISBN: (ebook)

Comentarios y preguntas (versión ESR - Colombia)

Envíe sus comentarios y preguntas sobre esta publicación a:
RENATA - Escuela Superior de Redes – ESR Colombia.
E-mail: esrcolombia@renata.edu.co
www.renata.edu.co
Bogotá D.C. - Colombia

Prólogo a la versión portuguesa

La Escuela Superior de Redes, ESR, es una unidad de la Rede Nacional de Ensino e Pesquisa, RNP, responsable por la difusión del conocimiento en Tecnologías de la Información y Comunicación, TIC. La ESR nace con la propuesta de ser formadora y diseminadora de las competencias en TIC para el cuerpo técnico – administrativo de las universidades federales, escuelas técnicas y unidades federales de investigación. Su misión fundamental es realizar la capacitación técnica del cuerpo funcional de las organizaciones usuarias de la RNP, para el ejercicio de las competencias aplicables al uso eficaz y eficiente de las TIC.

La ESR ofrece decenas de cursos en áreas temáticas como: administración y proyecto de redes, administración de sistemas, seguridad, medios de soporte a la colaboración digital de gobierno de TI.

La ESR también participa en diversos proyectos de interés público, como la elaboración y ejecución de planes de capacitación para la formación de multiplicadores para proyectos educativos como: formación en el uso de video conferencia para la Universidad Abierta de Brasil, UAB, formación de soporte técnico de laboratorios del Proinfo y creación de un conjunto de cartillas sobre redes inalámbricas para el programa Un Computador por Alumno, UCA.

Prólogo a la versión en castellano

La Red Nacional Académica de Tecnología Avanzada, RENATA, tiene el gusto de presentarle a la comunidad académica, científica, tecnológica y empresarial del país, la Escuela Superior de Redes (ESR) RENATA Colombia, esfuerzo de colaboración con la Rede Nacional de Ensino y Pesquisa, RNP Brasil e Instituciones de Educación Superior en Colombia, como parte de nuestra estrategia STAR (Servicios de Tecnología Avanzada RENATA).

Nuestro objetivo es la formación de alto nivel en competencias TIC para todo el personal técnico, administrativo y académico del país, tanto de instituciones conectadas como no conectadas a RENATA de modo tal que se permita incrementar y mejorar la eficiencia en el uso de las tecnologías de la información y las comunicaciones para el trabajo colaborativo en Colombia.

Es también este el espacio para agradecerle a RNP y las universidades del país que han participado en la construcción de este programa académico, junto con los profesores y técnicos que pusieron todo de sí para llevar a buen puerto esta iniciativa.

RENATA los invita a todos a sacarle el mayor provecho a este proceso formativo y a beneficiarse de todo el potencial y los Servicios de Tecnología Avanzada RENATA, STAR.

RENATA es la red nacional de investigación y educación de Colombia que conecta, articula e integra a los actores del Sistema Nacional de Ciencia Tecnología e Innovación (SNCTI) entre sí y con el mundo, a través del suministro de servicios, herramientas e infraestructura tecnológica para contribuir al mejoramiento del nivel de productividad, efectividad y competitividad de la producción científica y académica del país.

Metodología de la ESR

La filosofía pedagógica y la metodología que orientan los cursos de la ESR están basadas en el aprendizaje como construcción del conocimiento por medio de la resolución de problemas típicos de la realidad del profesional en formación. Los resultados obtenidos en los cursos de naturaleza teórico-práctica son optimizados, pues el instructor, ayudado por el material didáctico, actúa no solo como un expositor de conceptos e información, pero si principalmente como orientador del alumno en la ejecución de las actividades contextualizadas en las situaciones de su cotidiano profesional.

El aprendizaje es entendido como una respuesta del alumno al desafío de situaciones-problemas semejantes a las encontradas en la práctica profesional, que son superadas por medio del análisis, síntesis, juzgamiento, pensamiento crítico y construcción de hipótesis para la solución del problema, en abordajes orientadas al desarrollo de competencias.

Así, el instructor tiene participación activa y dialogada como orientador del alumno para las actividades en el laboratorio. Inclusive la presentación de la teoría al inicio de la sesión de aprendizaje no es considerada una simple exposición de conceptos e información. El instructor busca incentivar la participación de los alumnos continuamente.

Las sesiones de aprendizaje en las que se realizan la presentación de contenidos y la realización de las actividades prácticas tienen formato presencial y esencialmente práctico, utilizando técnicas de estudio dirigido individual, trabajo en equipo y prácticas orientadas al contexto de actuación del futuro especialista que se pretende formar.

Las sesiones de aprendizaje se desarrollan en tres etapas, con mayor dedicación a las actividades prácticas, conforme a la siguiente descripción:

Primera etapa: presentación de la teoría y solución de dudas (de 60 a 90 minutos).

El instructor presenta, de manera sintética, los conceptos teóricos correspondientes al tema de la sesión de aprendizaje, con ayuda de diapositivas en formato Power Point. El instructor formula interrogantes sobre el contenido de las diapositivas en lugar de solo presentarlas, animando al grupo a la participación y la reflexión. Eso evita que las presentaciones sean monótonas y que el alumno se coloque en actitud pasiva, lo que reduciría el aprendizaje.

Segunda etapa: actividades prácticas de aprendizaje (de 120 a 150 minutos)
Esta etapa es la esencia de los cursos de la ESR. La mayoría de las actividades de los cursos es asincrónica y realizada en grupos de dos alumnos, que siguen el ritmo de la guía de actividades propuesta en el libro de apoyo. El instructor y el monitor circulan entre los grupos para solucionar las dudas y ofrecer explicaciones complementarias.

Tercera etapa: discusión de las actividades realizadas (30 minutos)
El instructor comenta cada actividad, presentando una de las soluciones posibles, prefiriendo aquellas que generan mayor dificultad y polémica. Los alumnos son invitados a comentar las soluciones encontradas y el instructor retoma tópicos que hayan generado dudas, estimulando la participación de los alumnos. El instructor siempre estimula a los alumnos a encontrar soluciones alternativas a las sugeridas por él y por sus colegas, en caso que existan, y a comentarlas.

Sobre el curso

El objetivo del curso es desarrollar las habilidades necesarias para la aplicación de la gestión de seguridad de la información. Durante el curso el participante se introduce a los conceptos y definiciones básicas de la seguridad de la información, recibiendo de la ESR las normas de seguridad NTC ISO / IEC 27001 y NTC ISO/ IEC 27002. Con base en éstas va a entender los conceptos de la política de seguridad y de la gestión del riesgo y va a conocer las buenas prácticas para la seguridad de los recursos humanos y computacionales, la seguridad física y los derechos digitales. El curso garantiza al participante todo el conocimiento necesario para iniciar un proceso de implementación de la gestión de la seguridad de la información en su institución.

A quienes se destina

El curso está dirigido a directivos y profesionales de las TIC que necesitan adquirir competencias en el ámbito de la seguridad de la información. También pueden beneficiarse los profesionales que deseen aplicar los conocimientos en la gestión de seguridad de la información en cualquier organización.

Convenciones utilizadas en el libro

Las siguientes son convenciones tipográficas usadas en este libro:

Indica una referencia complementaria disponible en internet.

Indica un alerta o precaución a tener en cuenta.

Indica cuestionamientos que estimulan la reflexión o presentan contenido de apoyo para la comprensión del tema tratado.

Indica un documento como referencia complementaria.

Sobre los autores de la versión portuguesa

Flávia Estélia Silva Coelho con una Maestría en Informática de la Universidad Federal de Campina Grande y profesional en Ciencias de la Computación,. Desde el 2001, trabaja en la enseñanza de Pregrado y Postgrado Lato Sensu, en proyectos de investigación y desarrollo en las áreas de computación distribuida y seguridad de la información. Es profesora en la Universidad Federal Rural de Semi-Árido (UFERSA), desde el año 2009, y Java Champion (Oracle), desde 2006.

Luiz Geraldo Segadas de Araújo con Especialización en Gestión de la Seguridad de la Información, Redes de Computadores e Infraestructura Computacional. Trabajó para varias empresas, entre ellas la Fundación Petros, y ha trabajado también como consultor, especialmente para el BNDES y TBG. Tiene experiencia en la docencia, fue profesor de la Universidad Estácio de Sá y de Infnet, también instructor en RNP / ESR. Tiene un amplio conocimiento de las normas, sobre todo en la ISO / IEC 27001 y 27002. Profesional en Sistemas de la Información de la PUC-RJ, Postgrado en Redes de Computadoras de la UFRJ y Master en Administración de Empresas en la PUC-RJ. Tiene las certificaciones CISSP, CISA y CISM, y está capacitado en la planificación, el desarrollo de políticas de seguridad, normas, análisis de riesgo, diagnóstico y auditoría. Actualmente vive en Canadá.

Edson Kowask Bezerra profesional del área de seguridad de la información y gobierno de información, con más de quince años como auditor líder de calidad, investigador, director de proyectos y director técnico en varios proyectos de gestión de riesgos, la gestión de la seguridad de la información, continuidad del negocio, PCI, auditoría y recuperación de desastres en las grandes empresas de telecomunicaciones, financiera, energía, industria y empresas del sector del gobierno. Con amplia experiencia en las áreas de seguridad. También ha actuado como conferencista en importantes eventos en Brasil y también como instructor de formación en los temas de seguridad y gobierno. Es profesor y coordinador de cursos de postgrado en el área de seguridad de la información, la gestión integrada, la innovación y las tecnologías web. Hoy se desempeña como Coordinador Académico de Seguridad y Gobierno de las TI de la Escuela Superior de Redes.

Sobre el autor de la versión adaptada y ampliada

Hernando Peña Villamil, Magíster en Teleinformática de la Universidad Distrital Francisco José de Caldas e Ingeniero Electrónico. Directivo de Tecnología con más de 20 de años de experiencia, liderando proyectos de las TICs con certificaciones internacionales PMP, CobiT FC, ITIL FC e ISO 27001 IA. Vicepresidente Financiero del PMI-Colombia y Director de Membresía de ISACA-Colombia. Catedrático de posgrado en Gobierno de Tecnología de la Información y Gerencia de Proyectos de las Universidades Nacional de Colombia, ICESI de Cali, Autónoma de Manizales, EAN, Militar y de La Salle. Miembro de los grupos de investigación TGI (Tendencias en Gestión e Innovación) y G3Pymes de la Universidad EAN. Desde el 2011 se desempeña como Consultor de gobierno de las TI.

Sobre la traducción para la versión adaptada y ampliada

Oscar Edwin Piamba Tulcán, Doctor en Ingeniería Mecánica de la Universidad Federal Fluminense, Magíster en Ingeniería Mecánica de la Universidad de los Andes con Especialización en Ciencias: Física de la misma Universidad e Ingeniero Mecánico de la Universidad Nacional de Colombia. Vinculado como profesor a la Facultad de Ingeniería de Universidad Nacional de Colombia desde el año 2000, se desempeña como Director Nacional de Información Académica desde 2010. Participa como docente en los programas de Doctorado en Ingeniería Mecánica, en el Doctorado en Ciencia y Tecnología de Materiales y en los programas de maestría y pregrado en Ingeniería Mecánica y Mecatrónica.

Tabla de Contenido

Capítulo

01

Fundamentos de la Seguridad de la Información

Objetivos

Explicar las definiciones más importantes y preocupaciones comunes a considerar en términos de seguridad de la información en las organizaciones, seleccionar servicios y controles para la seguridad de la información e identificar los factores críticos de éxito.

Conceptos

Servicios de seguridad, gestión de seguridad de la información, amenazas, vulnerabilidades, ataques y controles.

1.1 Tendencias en el área de la "gestión de seguridad de información"

La gestión de seguridad de la información viene evolucionando desde sus albores como norma ISO-17799 del año 2000, hasta convertirse en la familia ISO 27000 desde el 2005 pretendiendo ser una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información. Esta norma está dirigida a los responsables de iniciar, implantar o mantener la seguridad de la información de una organización.

La norma ISO 27001:2005 está orientada a establecer, implementar, operar, monitorear, analizar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, SGSI y está alineada con la norma ISO 9001 con el fin de apoyar la implementación y operación, consistente e integrada con sistemas de gestión relacionados. Es decir, consolidar diversos sistemas de gestión de las organizaciones en uno sólo sistema integrado, optimizando sus procesos y facilitando el tránsito de información entre ellos.

Recientemente, en octubre del 2013 se ha actualizado la norma de requisitos del SGSI denominada ISO27001:2013 así como también la norma del Código de Práctica del Sistema de Gestión de Seguridad de la Información denominada ISO27002:2013.

La edición 2013 de la norma ISO27001 proporciona un enfoque común y una estructura para las normas de los sistemas de gestión que se presta más fácilmente para la integración con otras normas de sistemas de gestión. La norma actualizada ISO-27001 cuenta con 114 controles en 14 categorías o dominios, en contraste con los 133 controles y 11 categorías contenidas en la edición 2005. Los requerimientos para el análisis de riesgos están alineados con la norma ISO 31000 para la gestión del riesgo.

La norma ISO-27002 proporciona las directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, considerando el entorno de riesgos de seguridad de la información de la organización. El nuevo código de prácticas ha sido alineado, en cuanto al número de controles, con los de la norma ISO/IEC 27001, así como la terminología con la de la norma ISO/IEC 27000. Refleja la estructura del Anexo A de la norma ISO/IEC 27001:2013.

1.2 ¿Por qué preocuparse por la seguridad?

Problemas comunes:

- Destrucción de la información y otros recursos.
- Modificación o distorsión de información.
- Robo, eliminación o pérdida de información u otros recursos.
- La revelación de información.
- La interrupción de los servicios.

Ejercicio de nivelación - fundamentos de la seguridad de la información

- ¿Qué es seguridad para usted?
- ¿Qué entiende por seguridad de la información?

La seguridad de la información es fundamental para la supervivencia de las organizaciones en la era de la información. Varios problemas están involucrados, dado que la sociedad depende de la información almacenada en los sistemas informáticos para la toma de decisiones en las empresas, entidades del gobierno, entre otros contextos organizacionales.

La información puede existir en varios formatos: impresa, almacenada electrónicamente, hablada, transmitida por correo convencional de voz o electrónico, etc. Cualquiera que sea el formato o medio de transmisión o almacenamiento, se recomienda proteger la información de manera adecuada. Por lo tanto, es responsabilidad de la seguridad de la información protegerla de los diversos tipos de amenazas para garantizar

la continuidad del negocio, minimizar el riesgo y maximizar el retorno sobre la inversión.

Afortunadamente, hay una conciencia creciente de organizaciones de todo el valor y la vulnerabilidad de las actividades de sus activos con respecto a la seguridad. Hoy en día, la seguridad de la información es crucial para asegurar la competitividad, la rentabilidad, el cumplimiento de los requerimientos legales y la imagen de la organización en el mercado de las organizaciones, tanto en el sector público como en el sector privado. En tales contextos, la seguridad de la información es un componente que viabiliza negocios, tales como e-government (gobierno electrónico) y el e-commerce (comercio electrónico).

1.3 Definiciones

La seguridad de la información incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad.

De acuerdo con la norma ISO/IEC 27002:2007, la seguridad de la información es la protección de la información contra los diversos tipos de amenazas para garantizar la continuidad del negocio, minimizando los riesgos y maximizando el retorno sobre la inversión y las oportunidades de negocio. La seguridad de la información se obtiene como resultado de la implementación de un conjunto de controles, que comprenden políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software.

En particular, los controles deben ser establecidos, implementados, monitoreados, evaluados y mejorados continuamente con el fin de cumplir con los objetivos del negocio y la seguridad de la organización. La identificación de los controles adecuados requiere una planificación detallada. A continuación se especifican algunos conceptos:

- **Incidente de seguridad:** corresponde a cualquier evento adverso relacionado con la seguridad, por ejemplo, ataques de denegación de servicio (*Denial of Service*, DoS), robo de información, fuga y la obtención de un acceso no autorizado a la información.
- **Activo:** cualquier elemento que tenga valor para la organización y su negocio. Algunos ejemplos: bases de datos, software, equipos (computadores, *notebooks*), servidores, dispositivos de red (*routers, switches*, etc), personas, procesos y servicios.

- **Amenaza:** cualquier evento que explote vulnerabilidades. Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización (véase el punto 2.16 NTC ISO/IEC 27002:2007).
- **Vulnerabilidad:** cualquier debilidad que puede ser explotada y ponga en peligro la seguridad de los sistemas y datos. Fragilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas (véase el punto 2.17 NTC ISO / IEC 27002:2007). Las vulnerabilidades son fallas que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades. A partir de esta falla, las vulnerabilidades son explotadas por amenazas que cuando se materializan, causan daños al computador, a la organización o a los datos personales.
- **Riesgo:** combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización.
- **Ataque:** cualquier acción que comprometa la seguridad de una organización.
- **Impacto:** resultado evaluado de un evento en particular.

Ejercicio de refuerzo – definiciones

- ¿Explique qué son activos para usted?
- ¿Cómo explicaría en su organización el término "vulnerabilidad"?

1.4 Modelos de ataque

Hay cuatro modelos posibles de ataque:

- **Interrupción:** cuando un activo se destruye o queda indisponible (o inutilizable), caracterizando un ataque contra la disponibilidad. Por ejemplo, la destrucción de un disco duro.
- **Interceptación:** cuando se accede a un activo por un tercero no autorizado (persona o programa del computador), caracterizando un ataque contra la confidencialidad. Por ejemplo, la copia no autorizada de archivos o programas.

» **Modificación:** cuando se accede a un activo por un tercero no autorizado (persona o programa del computador) y se modifica, materializando un ataque contra la integridad. Por ejemplo, cambio de los valores en un archivo de datos.
» **Fabricación:** cuando una parte no autorizada (persona o programa del computador) inserta objetos falsificados en un activo, configurando un ataque contra la autenticidad. Por ejemplo, la adición de registros en un archivo.

En la Figura 1, se observa el flujo normal de la información de una fuente a un destino (a). En secuencia, se presentan cada uno de estos modelos de posibles ataques: una interrupción (b), intercepción (c), modificación (d) y fabricación (e).

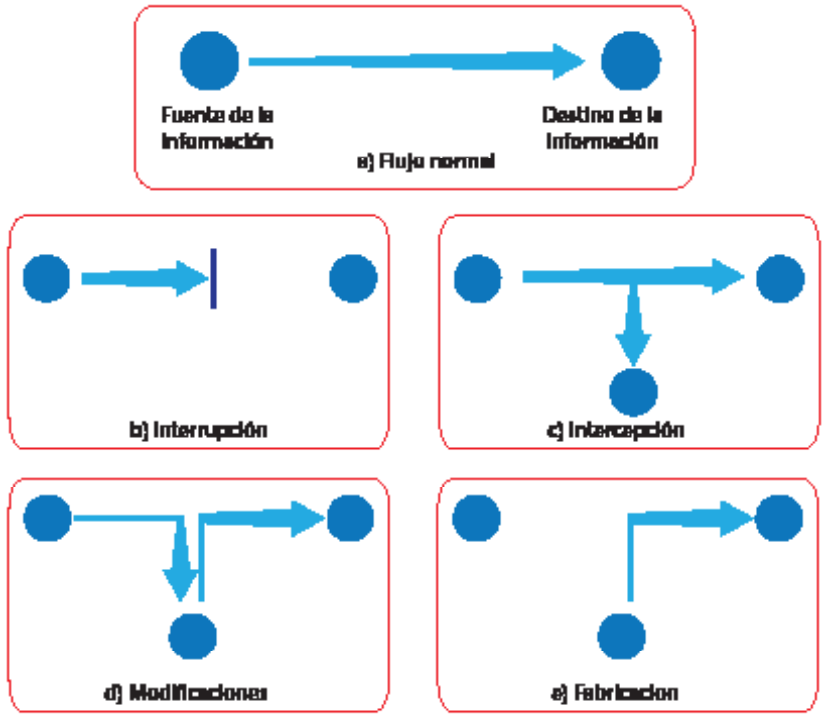


Figura 1. Modelos de ataque

Ejercicio de refuerzo - modelos de ataque

» Explique el modelo de ataque de la intercepción.

1.5 Formas de ataque

El ataque es un acto deliberado de tratar de esquivar los controles de seguridad con el objetivo de explotar las vulnerabilidades. Existen los siguientes tipos de ataque:

- **Ataques pasivos:** ataques basados en escuchar y monitorear las transmisiones, con el fin de obtener la información que se está transmitiendo. Escuchar una conversación telefónica es un ejemplo de esta categoría. Los ataques de esta categoría son difíciles de detectar debido a que no implica cambios en los datos, sin embargo, son posibles de prevenir con el uso de la criptografía.
- **Ataques activos:** involucran la modificación de datos, la creación de objetos falsos o negación de servicio, y tienen las propiedades opuestas de ataques pasivos. Son ataques difíciles de prevenir debido a la necesidad de una protección completa de todas las instalaciones de comunicaciones y procesamiento, durante todo el tiempo. Por lo tanto, es posible detectarlos y aplicar una medida para la recuperación de los perjuicios causados.

Ejercicio de refuerzo - formas de ataque

- Explique cómo ocurriría un ataque activo en el entorno de su organización.

1.6 Arquitectura de seguridad

Arquitectura de seguridad propuesto por el modelo *Open Systems Interconnection*, OSI (Interconexión de Sistemas Abiertos) definida en la Norma ISO 7498-2 establece los siguientes objetivos y requisitos de seguridad:

- Proteger los datos contra modificaciones no autorizadas.
- Proteger los datos contra pérdida / robo / hurto.
- Proteger los datos contra toda divulgación no autorizada.
- Asegurar la identidad del remitente correcto de los datos.
- Asegurar la identidad del destinatario correcto de los datos.

1.7 Servicios de seguridad

En este tema, son tratados los objetivos y las categorías de los servicios de seguridad que son considerados en el contexto de seguridad de la información. De acuerdo con la norma ISO 7498-2, que incluye los aspectos relacionados con la seguridad en el modelo de OSI, los servicios de seguridad son medidas preventivas elegidas para hacer frente a las amenazas identificadas. Los servicios de seguridad aumentan la seguridad de la información frente a ataques haciendo uso de uno o más mecanismos de seguridad. En la literatura estos servicios también son citados como los principios básicos de seguridad.

Los servicios y mecanismos de seguridad deben aplicarse con el fin de cumplir con los requisitos de seguridad de la organización, teniendo en cuenta el equilibrio entre las necesidades de seguridad y los costos respectivos. En particular, para identificar y dar prioridad a los servicios de seguridad, es esencial analizar los riesgos y los impactos probables que comprenden a toda la organización en cuestión.

- **Confidencialidad:** comprende la protección de los datos transmitidos contra ataques pasivos, es decir, el acceso no autorizado, que incluirá medidas tales como el control de acceso y encriptación. La pérdida de la confidencialidad se produce cuando hay una violación de la confidencialidad de cierta información (por ejemplo, la contraseña de un usuario o administrador del sistema) permitiendo que quede expuesta la información restringida, las cuales estaban disponibles sólo a un determinado grupo de usuarios.
- **Autenticidad:** está interesada en garantizar que la comunicación sea auténtica, es decir, origen y destino pueden verificar la identidad de la otra parte implicada en la comunicación, con el fin de confirmar que la otra parte es quien dice ser. El origen y el destino son normalmente usuarios, dispositivos o procesos.
- **Integridad:** es la garantía contra ataques activos a través de los cambios o de remociones no autorizadas. Es importante utilizar un esquema que permite la verificación de la integridad de los datos almacenados y su transmisión. La integridad puede ser considerada bajo dos aspectos: servicio sin y con recuperación. Una vez que los ataques activos son considerados en su contexto, la detección, en lugar de la prevención, es lo que importa, así, si se detecta un peligro para la integridad, puede ser reportado y el mecanismo de recuperación se activa inmediatamente. La integridad es también un prerrequisito para otros servicios de seguridad. Por ejemplo, si la integridad de un sistema de control de acceso a un sistema operativo es violada, también se viola

la confidencialidad de sus archivos. La pérdida de la integridad se produce en un momento en que cierta información está expuesta a la manipulación por personal no autorizado, que hace cambios que no fueron aprobados y no están bajo el control del propietario de la información (corporativo o privado).

- **No repudio:** comprende el servicio que impide a una fuente o destino negar la transmisión de mensajes, es decir, cuando se envía el mensaje dado, el destino puede demostrar que éste fue enviado realmente por determinado origen y viceversa.
- **Conformidad:** deber de cumplir y hacer cumplir las regulaciones internas y externas impuestas a las actividades de la organización. Estar en conformidad es estar de acuerdo, siguiendo y haciendo cumplir las leyes y reglamentos internos y externos.
- **Control de acceso:** trata de limitar y controlar el acceso lógico / físico a los activos de una organización a través del proceso de identificación, autenticación y autorización, con el fin de proteger los recursos contra el acceso no autorizado.
- **Disponibilidad:** determina que los recursos estén disponibles para el acceso por parte de entidades autorizadas, siempre que lo soliciten, representando la protección contra la pérdida o degradación. La pérdida de la disponibilidad sucede cuando la información deja de estar accesible para aquellos que la necesitan. Sería el caso de pérdida de comunicación con un sistema importante para la organización, que ocurrió al caer un servidor o una aplicación crítica para el negocio, que presentó una falla debido a un error causado por motivo interno o externo al equipo o por la acción de personas no autorizadas, con o sin intención maliciosa.

Ejercicio de refuerzo - servicios de seguridad

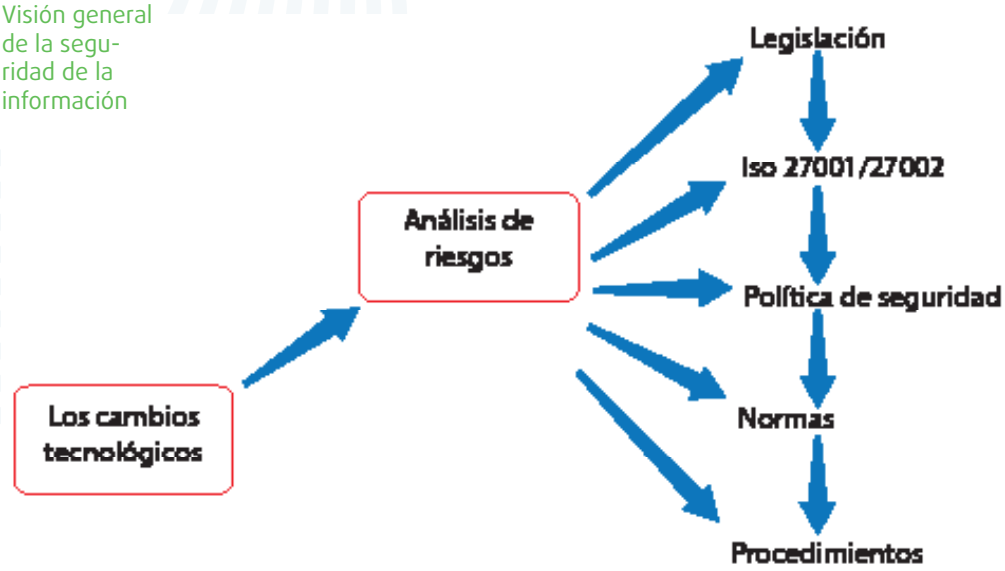
- Explique cómo su organización protege la confidencialidad
- Explique qué viene a ser autenticidad e integridad.

1.8 Seguridad de la información

En este tema, se detallan los principales aspectos relacionados con la gestión de la seguridad de la información, con la presentación de un panorama general de las preocupaciones, responsabilidades y actividades involucradas.

La Figura 2 presenta una visión general de la seguridad de la información. Los cambios tecnológicos son una presencia constante en la vida diaria de la organización. Estos cambios pueden hacer que surjan nuevas vulnerabilidades y riesgos, o agravar los ya existentes, por lo cual deben ir acompañados de una evaluación de riesgos dinámica y actualizada, lo que permite el levantamiento de los niveles de riesgo y la forma de tratarlos.

Figura 2.
Visión general de la seguridad de la información



Al mismo tiempo, es necesario conocer las leyes que la organización está obligada a seguir y recopilar los requisitos de seguridad necesarios para cumplir con ella, y a partir de estos requisitos legales, identificar los controles necesarios y los designados por el análisis de riesgos, con el uso de las normas de seguridad. A partir de los controles identificados, es necesario generar políticas, normas y procedimientos para la aplicación de los controles.

1.9 Preparando a la organización

Antes de pensar en la gestión de la seguridad de la información en una organización, hay que tener en cuenta las respuestas a las siguientes preguntas:

- ¿Qué hay que proteger? Los activos de la organización requieren protección.
- ¿Contra qué o quién? ¿Cuáles son las amenazas que pueden afectar a la organización y cómo y quién puede explotar estas amenazas?
- ¿Cuál es la importancia de cada recurso? Cada recurso de la información participa en el proceso de negocio de la organización.

Proceso de negocio: conjunto de acciones y actividades que coexisten e interactúan de una manera lógica y coherente para desarrollar un entregable (producto) que cumpla con los requisitos de calidad y las expectativas del cliente, ya sea interno o externo.

- ¿Cuál es el grado de protección deseado?
- ¿Qué requisitos de protección el negocio exige y qué nivel de protección es necesario?
- ¿Cuánto tiempo, recursos financieros y humanos, usted desea gastar para alcanzar los objetivos de seguridad deseados?
- ¿Qué recursos están disponibles para los objetivos de seguridad y qué se puede hacer con los recursos existentes?
- ¿Cuáles son las expectativas de los directivos, clientes y usuarios en materia de seguridad de la información?
- ¿Qué esperan de la seguridad de la información para el negocio de la organización?

Con las respuestas a estas preguntas, usted puede continuar con el proceso de establecimiento de la seguridad de la información y su gestión en la organización.

1.10 Requisitos de seguridad

Hay tres fuentes principales a tener en cuenta al establecer los requisitos de seguridad de la información de una organización:

- **Evaluación/análisis de riesgos:** considera los objetivos y estrategias de negocio de la organización, lo que resulta en la identificación de las vulnerabilidades y las amenazas a los activos. En este contexto, se tiene en cuenta la probabilidad de ocurrencia de las amenazas y el impacto en el negocio.
- **Legislación vigente:** estatutos, reglamentos y las cláusulas contractuales que deben cumplirse para la organización, sus socios, subcontratistas y proveedores.
- **Conjunto de principios:** los objetivos y requisitos de negocios para el procesamiento de datos que la organización debe definir para dar soporte a sus operaciones.

Para mayor información consulte la norma NTC ISO/IEC 27002:2007.

1.11 Análisis/evaluación de riesgos

En el análisis/evaluación de riesgo, los gastos en los controles deben ser equilibrados en función del impacto que causará posibles fallas de seguridad en los negocios. Por lo tanto, se debe realizar periódicamente el análisis/evaluación con el fin de contemplar cambios en la organización.

Estos resultados ayudarán a determinar y direccionar las acciones gerenciales y las prioridades para la gestión del riesgo de seguridad de la información. La evaluación compara el riesgo estimado con los criterios predefinidos para determinar la importancia o el valor del riesgo para la organización.

Más información consulte la norma NTC ISO/IEC 27005:2008

1.12 Selección de controles

Tras la identificación de los requisitos de seguridad, el análisis/evaluación de riesgos y la toma de decisiones con respecto al tratamiento del riesgo en una organización, se pueden finalmente, seleccionar e implementar los controles adecuados.

Los controles son medidas o conjunto de medidas adoptadas para hacer frente a las vulnerabilidades y reducir el riesgo de incidentes de seguridad de la información. El control, también conocido como contramedida, es cualquier mecanismo útil para gestionar los riesgos, incluyendo las políticas, procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal.

Los controles se pueden seleccionar a partir de normas preestablecidos (por ejemplo, las normas NTC ISO/IEC 27002:2007 Y NTC ISO / IEC 27001:2006) o de un conjunto de controles específicos de la organización. En particular, los controles seleccionados deben estar de acuerdo con las leyes y regulaciones nacionales e internacionales vigentes relevantes para la seguridad de la información y para los negocios de la organización.

Algunos ejemplos de control:

- Las barreras, puertas, carteles de "prohibido entrar", torniquetes;
- Tarjetas de control de visitantes, circuito cerrado de televisión;
- contraseñas, cerraduras, controles biométricos;
- Las políticas de seguridad, manual de responsabilidad, entrenamiento;
- Antivirus, copias de seguridad, control de acceso lógico.

Control biométrico:

El uso de la biometría para identificar o verificar el acceso a recursos tales como computadores, *notebooks*, teléfonos inteligentes, redes de computadores, aplicaciones, bases de datos y otros hardware y software que necesitan tener su acceso protegido. La biometría es el uso de las características físicas o de comportamiento de las personas como una forma de identificarlas.

Ejercicio de refuerzo - selección de controles

» Explique qué son los controles.

1.13 Los controles de seguridad de la información

El control, por definición, es una forma de gestionar el riesgo y puede incluir políticas, procedimientos, directrices y prácticas que pueden ser de carácter administrativo, técnico, legal o de gestión. Algunos controles pueden ser considerados como "primeros pasos" para la seguridad de la información en las organizaciones, con base en requisitos legales y / o mejores prácticas para la seguridad de la información.

Desde el punto de vista legal, existen controles considerados fundamentales y dependen de la legislación vigente, es decir:

» Protección de datos y privacidad de la información personal;
» Protección de los registros de la organización;
» Derechos de propiedad intelectual.

Los controles considerados buenas prácticas para la seguridad de la información son:

» Documento de la política de seguridad de la información;
» Asignación de responsabilidades para la seguridad de la información;
» Sensibilización, educación y capacitación en seguridad de la información;
» Procesamiento correcto en las aplicaciones;
» Gestión de las vulnerabilidades técnicas;
» Gestión de la continuidad del negocio;
» Gestión de incidentes de seguridad de la información.

Es importante que la selección o no de un control determinado sea una acción basada en los riesgos específicos de la organización. Por lo tanto, tenga en cuenta los controles designados como punto de partida, dado que no sustituyen a la selección de los controles basados en el análisis/ evaluación de riesgos.

Es notorio, sin embargo, la concientización de que una política de seguridad de la información no debe ser definida en términos generales. Las

organizaciones deben ser analizadas caso por caso, con el fin de identificar sus necesidades de seguridad y así desarrollar e implementar una política adecuada. Además, la política debe asignar derechos y responsabilidades a las entidades que tienen que ver directamente con la información y recursos informáticos de las organizaciones. Por lo que cualquier evento que resulte en violación de la política se considera un incidente de seguridad.

Otra cuestión a considerar es la gestión de la continuidad del negocio, lo que tiene que ver con los planes de contingencia y continuidad, con énfasis en la planeación para asegurar la recuperación de desastres.

Ejercicio de refuerzo - los controles de seguridad de la información

- ¿Cuáles son los controles que se consideran esenciales desde el punto de vista legal?
- En su organización, ¿qué controles aplicados se consideran como mejores prácticas?

1.14 Elementos relevantes para la seguridad de la información

La gestión de seguridad de la información fomenta la adopción de políticas, procedimientos, directrices y otros elementos pertinentes cuyo alcance debe comprender la gestión del riesgo sobre la base de costo / beneficio para la organización.

En este contexto, para la gestión de la seguridad de la información, los elementos siguientes son relevantes:

- Política de seguridad de la información.
- Seguridad organizacional.
- Gestión de activos.
- Seguridad de recursos humanos.
- La seguridad física y del ambiente.
- Gestión de las operaciones y comunicaciones.
- Control de acceso.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.

Todos los elementos son tratados en detalle en la norma NTC ISO/IEC 27002:2007 y se explicarán en este curso.

1.15 Actividades relacionadas

Actividades adicionales consideradas en el ámbito de la gestión de seguridad de la información:

- Gestión de la seguridad de los sistemas, que abarca todos los aspectos de la seguridad de los sistemas de una organización, tales como la administración de la política de seguridad, procedimientos de recuperación de desastres, entre otros. Es responsabilidad de esta gestión actualizarse constantemente con respecto a los problemas, los riesgos y las soluciones de seguridad más recientes.
- Gestión de los servicios de seguridad, incluyendo la selección de los mecanismos de seguridad más adecuados para atenderlos.
- Gestión de los mecanismos de seguridad disponibles para cumplir los requisitos de seguridad de la organización.
- Gestión de la auditoría de seguridad, revisión y verificación de registros y eventos de seguridad, con el objetivo de evaluar la idoneidad de los controles del sistema, su adhesión a la política de seguridad, y recomendar cambios apropiados / necesarios a los controles empleados en la organización.

1.16 Factores críticos para el éxito de la seguridad de la información

Los siguientes son algunos de los factores que son críticos para el éxito de la seguridad de la información en las organizaciones:

- La política de seguridad de la información, los objetivos y las prácticas deben reflejar los objetivos de negocio de la organización.
- El enfoque y la estructura que han sido adoptados para la ejecución, el mantenimiento, el seguimiento y la mejora de la seguridad de la información deben ser compatibles con la cultura de la organización.
- Todos los niveles gerenciales de la organización deben estar comprometidos y apoyar la seguridad de la información.

- Los requisitos de seguridad de la información, el análisis, la evaluación y la gestión del riesgo deben ser bien entendidos (en detalle).
- La seguridad de la información debe darse a conocer, de manera eficiente, a todas las entidades de la organización (presidentes, directores, gerentes, empleados, contratistas, etc.).
- Distribución y comunicación de directrices, políticas y normas para todas las partes involucradas
- Suministro de recursos financieros para la gestión de seguridad de la información.
- Suministro de sensibilización, entrenamiento y educación adecuadas.
- Establecimiento de un proceso eficiente para la gestión de incidentes de seguridad
- Implementación de un sistema de medición de la gestión de seguridad de la información.
- Todos los elementos de la política de seguridad deben ser distribuidos y comunicados a las entidades de la organización.
- Los recursos financieros se deben proporcionar para la gestión de seguridad de la información.
- Medios de sensibilización, formación y educación adecuada deben ser provistos.
- Se debe establecer un procedimiento eficaz para la gestión de incidentes de seguridad de la información.
- Se debe implementar un mecanismo para medir y evaluar la eficacia de la gestión de seguridad de la información, con las sugerencias de mejora posteriores (véase el punto 0.8 de la norma NTC-ISO/IEC 27002:2007).

La gestión del riesgo

Involucra actividades para dirigir y controlar una organización en términos de riesgos. Por lo tanto, comprende el análisis, la evaluación, el tratamiento y la aceptación de los riesgos.

Capítulo

02

Código de práctica

Objetivos

Conocer la norma NTC-ISO/IEC 27002:2007 y seleccionar, relacionar y combinar sus controles.

Conceptos

Estructura y secciones de la norma NTC-ISO/IEC 27002:2007 y sus objetivos.

2.1 Estructura de la norma

La norma NTC-ISO/IEC 27002:2007 fue preparada para servir como una guía práctica para el desarrollo y la aplicación de los procedimientos y controles de seguridad de la información en una organización.

Ejercicio de nivelación - fundamentos de la seguridad de la información

» ¿Qué entiende usted por código de práctica?

Está estructurada para proporcionar un código de buenas prácticas para la gestión de la seguridad, la norma está organizada en capítulos de 0 a 15. En los capítulos 0-4 se presentan los temas de introducción (0), el objetivo de la norma (1), los términos y las definiciones adoptadas por la norma (2), la estructura de la norma (3) y el análisis / evaluación y tratamiento de riesgos (4), y son considerados como la sección introductoria.

Desde el capítulo 5, la norma llama a cada capítulo como sección. Por lo tanto, hay once secciones específicas que ofrecen los códigos de práctica de la gestión de la seguridad.

Para cada sección, existe al menos una categoría importante de la seguridad. Las once secciones forman un total de 39 categorías principales de seguridad. En la sección 3 de la norma son presentadas las secciones y la cantidad de categorías por cada sección. Cada categoría presenta un objetivo de control y uno o más controles que deben aplicarse con el fin de alcanzar el objetivo de control.

Hay 133 controles y ellos son los elementos que definen lo que la norma 27002 considera importante para un proceso de seguridad de la información. Los controles identificados por números (xx.xx.xx) son estructurados a través de:

- **Control:** descripción y definición de control;
- **Directrices para la implementación:** información auxiliar en la implementación del control;
- **Información adicional:** informaciones complementarias.

Todo el trabajo de este capítulo será desarrollado con el manejo y la lectura de los temas presentados en la norma NTC-ISO/IEC 27002:2007.

Figura 3. Secuencia estructural de la norma

En el sentido horario, se observa la secuencia estructural de la norma, destacando las once secciones de controles de seguridad de la información (secciones 5-15).

Más información se puede encontrar en la norma NTC-ISO/IEC 27002:2007

2.2 Sección 4: análisis/evaluación y tratamiento de los riesgos

Figura 4. Sección 4: análisis/ evaluación y tratamiento de riesgos

La sección 4 (análisis/evaluación y tratamiento de riesgos) es una sección introductoria que presenta objetivamente la importancia del análisis de riesgos para la organización, y las indicaciones generales de la forma en que debe hacerse.

2.3 Sección 5: política de seguridad

Figura 5. Sección 5.1: política de seguridad de la información

La sección 5 de la norma se refiere a la política de seguridad de la información. El objetivo de la categoría de control es proporcionar orientación y apoyo de gestión para la seguridad de la información, mediante el establecimiento de una política clara y objetiva, alineada con los objetivos de negocio de la organización. La sección 5 muestra la forma en que debe ser generado y actualizado el documento de la política.

Esta sección se compone de una categoría principal de seguridad (5.1: política de seguridad de la información) y dos controles (5.1.1 y 5.1.2).

El control 5.1.1 (documento de la política de seguridad de información) muestra, en las "Directrices para la implementación", lo que conviene que el documento de política contenga y la importancia de que sea comunicado a todos.

El control de 5.1.2 (análisis crítico de la política de seguridad de la información) presenta como corresponde que se realice el análisis crítico por parte de la dirección de la organización.

Ejercicio de refuerzo - sección 5: política de seguridad

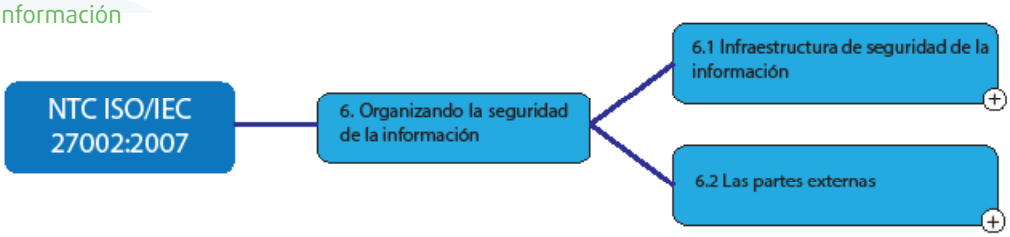
Utilizando la norma, explique:

- El objetivo de la categoría de control 5.1
- La letra b de las directrices para la implementación del control 5.1.1

2.4 Sección 6: organizando la seguridad de la información

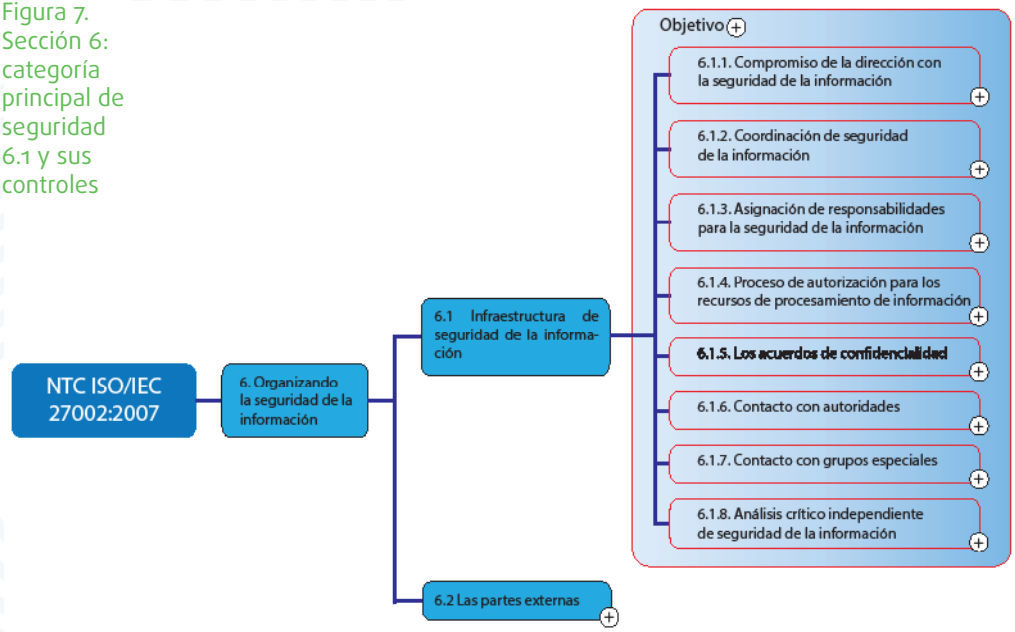
La sección 6 (organizando la seguridad de la información) tiene como objetivo presentar controles para gestionar la seguridad de la información dentro de la organización y también los controles para mantener la seguridad de los recursos de procesamiento de la información, cuando están disponibles para las partes externas. Como partes externas se entiende a todo aquel que no es parte efectiva de la estructura de la organización. Así, son ejemplos de partes externas los vendedores, proveedores, agencias gubernamentales, contratistas, proveedores de servicios temporales y los clientes, entre otros.

Figura 6.
Sección 6: organizando la seguridad de la información



En la sección 6 encontraremos los controles que deben aplicarse a la estructura funcional de la seguridad de la información. La sección 6 tiene dos categorías principales de seguridad: 6.1 (infraestructura de seguridad de la información) y 6.2 (las partes externas).

Figura 7.
Sección 6: categoría principal de seguridad 6.1 y sus controles



La categoría 6.1 (infraestructura de seguridad de la información) cuenta con ocho controles que se deben implementar. Estos controles, como puede verse en la norma, tratan de la estructura de la seguridad, sus procesos de autorización, confidencialidad, y los contactos con otros grupos.

Observe que el control 6.1.8 trata de nuevo el análisis crítico de la seguridad de la información. La seguridad de la información es parte de un proceso y debe ser analizada periódicamente, revisada y corregida para estar siempre al día con los requisitos de seguridad de la información.

Se recomendamos una lectura rápida de la categoría 6.1 de la norma NTC-ISO/IEC 27002:2007.

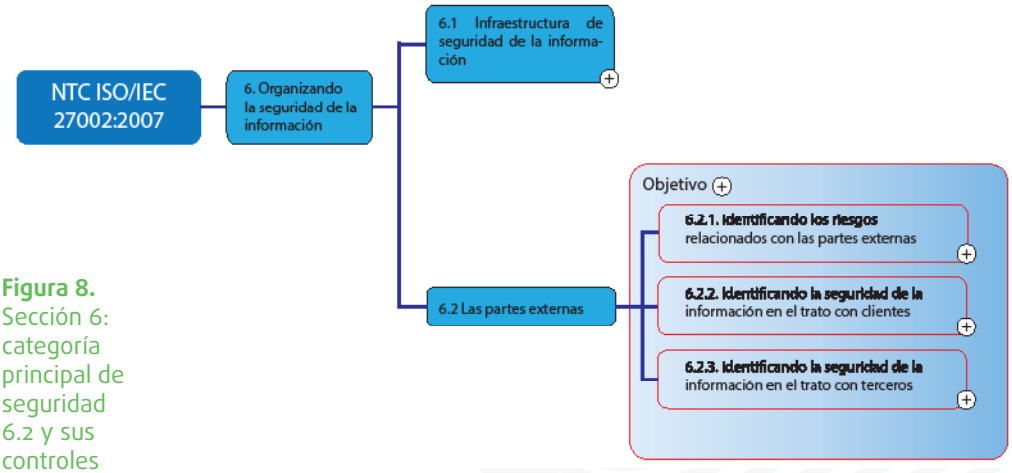


Figura 8. Sección 6: categoría principal de seguridad 6.2 y sus controles

La categoría 6.2 (partes externas) se refiere a los controles necesarios para la relación entre la organización y las partes externas que, en algún momento y por alguna razón del negocio, necesitan tener acceso a los recursos informáticos de la organización. Es una buena práctica identificar cada una de las partes externas que existen en la relación de negocios de la organización.

Tenga en cuenta los detalles de las directrices de implementación, que relaciona lo esencial a ser cumplido en la seguridad de la información.

Ejercicio de refuerzo - sección 6: organizando la seguridad de la información

Utilizando la norma, explique los controles

- 6.1.3
- 6.1.5
- 6.1.7

2.5 Sección 7: gestión de activos

En la sección 7 (gestión de activos) se presentan dos categorías principales de seguridad de la información:

- 7.1 (Responsabilidad de los activos): representa los controles que se aplican a la protección de los activos de la organización;
- 7.2 (Clasificación de la información): controles para la clasificación de la información, dándoles un nivel de seguridad adecuado.

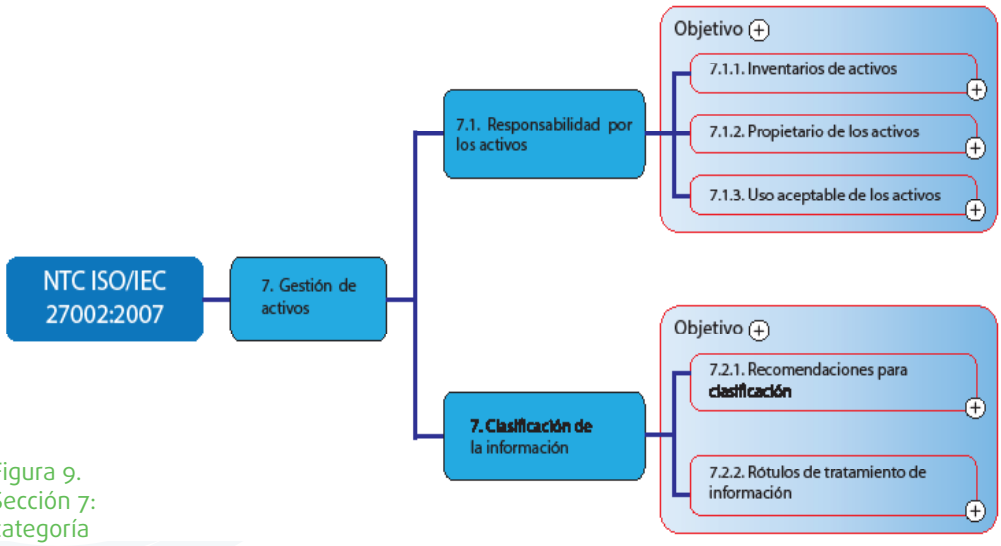


Figura 9. Sección 7: categoría principal de seguridad 7.1 y 7.2 con sus controles

La categoría 7.1 (Responsabilidad de los activos) tiene como objetivo alcanzar y mantener la protección adecuada de los activos de la organización, presentando los controles que se deben aplicar para el tratamiento de la seguridad de la información de los activos.

El control 7.1.1 de la norma, en "información adicional", describe algunos tipos de activos. La categoría 7.2 presenta los controles para el tratamiento de la seguridad de la información que deben ser aplicados.

Ejercicio de refuerzo - sección 7: gestión de activos

Utilizando la norma, explique los controles

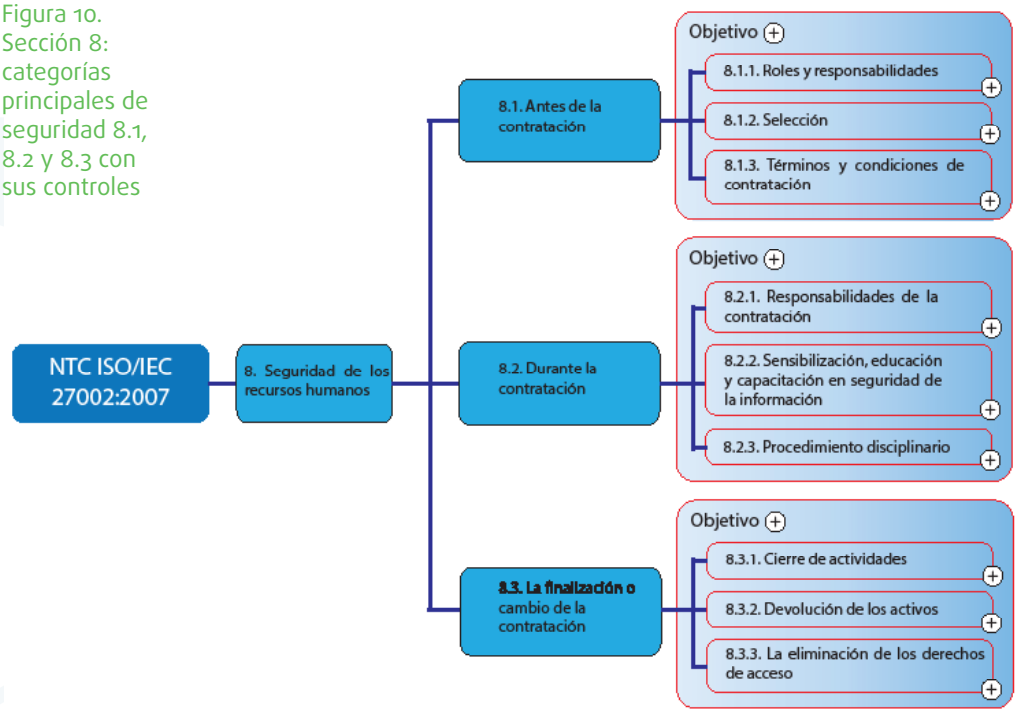
- 7.1.1
- 7.1.2
- 7.2.1

2.6 Sección 8: seguridad de los recursos humanos.

La sección 8 (seguridad de los recursos humanos) se ocupa de los controles de seguridad de la información durante el ciclo de vida de la prestación de servicio de profesionales en la organización. Estos controles están dispuestos por la norma en tres categorías:

- 8.1. Antes de la contratación;
- 8.2. Durante la contratación;
- 8.3. La finalización o cambio de la contratación.

Figura 10. Sección 8: categorías principales de seguridad 8.1, 8.2 y 8.3 con sus controles



Los controles en cada categoría se organizan dentro de las necesidades mínimas de seguridad que deben observarse en cada uno de ellos.

- Categoría 8.1 (controles responsabilidades): proceso de selección y condiciones de los contratos de recursos humanos;
- Categoría 8.2 (controles durante la prestación de los servicios propiamente dichos): en esta categoría están los controles de responsabilidades, la capacitación de los recursos humanos en seguridad de la información y los procedimientos disciplinarios, si se produce una violación de la seguridad de la información;
- Categoría 8.3 (controles específicos para el cierre o cambio de la contratación: cambio del área, de cargo, ascenso, etc.): en esta categoría se destacan los controles de devolución de los activos y la retirada de derechos de acceso.

Ejercicio de refuerzo - sección 8: seguridad en recursos humanos

Utilizando la norma, explique los controles

- 8.1.1
- 8.2.2
- 8.3.3

2.7 Sección 9: seguridad física y del entorno

Teniendo como objetivo del tratamiento de la seguridad física y del ambiente, la sección 9 (seguridad física y del ambiente) presenta dos categorías principales de seguridad de la información:

- 9.1. Áreas seguras;
- 9.2. Seguridad de los equipos.

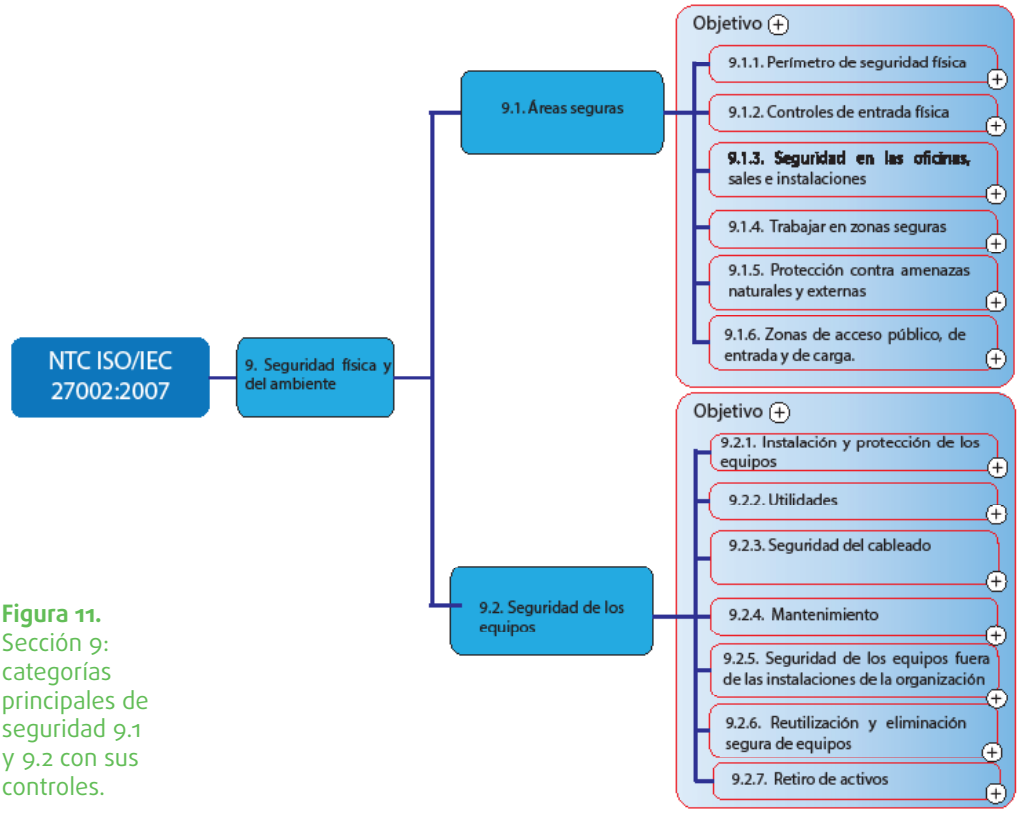


Figura 11. Sección 9: categorías principales de seguridad 9.1 y 9.2 con sus controles.

Los controles de seguridad de la categoría 9.1 (áreas seguras) se refieren específicamente a las necesidades de seguridad de acceso físico a las instalaciones. Presenta controles de seguridad para el perímetro físico, controles de entrada a las áreas internas y externas, zonas seguras, áreas de acceso público y de entrega de materiales.

En la categoría 9.2 (seguridad de equipos) están los controles de seguridad que se refieren a la protección física de los activos y su funcionamiento sin interrupciones. Es en esta categoría donde se encuentran los controles para la instalación de equipos, suministro de energía, aire acondicionado, mantenimiento de activos, la reutilización y la venta/eliminación de los activos.

Ejercicio de refuerzo - sección 9: seguridad física y del entorno

Utilizando la norma, explique los controles

- 9.1.2
- 9.1.4
- 9.2.5

2.8 Sección 10: gestión de operaciones y comunicaciones

La sección 10 (gestión de las operaciones y comunicaciones) es la sección más grande de la norma, se ocupa de las operaciones de los servicios tecnológicos de la organización. Esta sección tiene diez categorías principales de seguridad de la información, y cada uno de ellas cuenta con controles que deben ser aplicados en el día a día de las operaciones y las comunicaciones de la organización. Es la sección que muestra los controles de seguridad relacionados con la mayoría de las vulnerabilidades vinculadas a los aspectos operativos cotidianos en el área de las Tecnologías de la Información y las Comunicaciones, TICs.

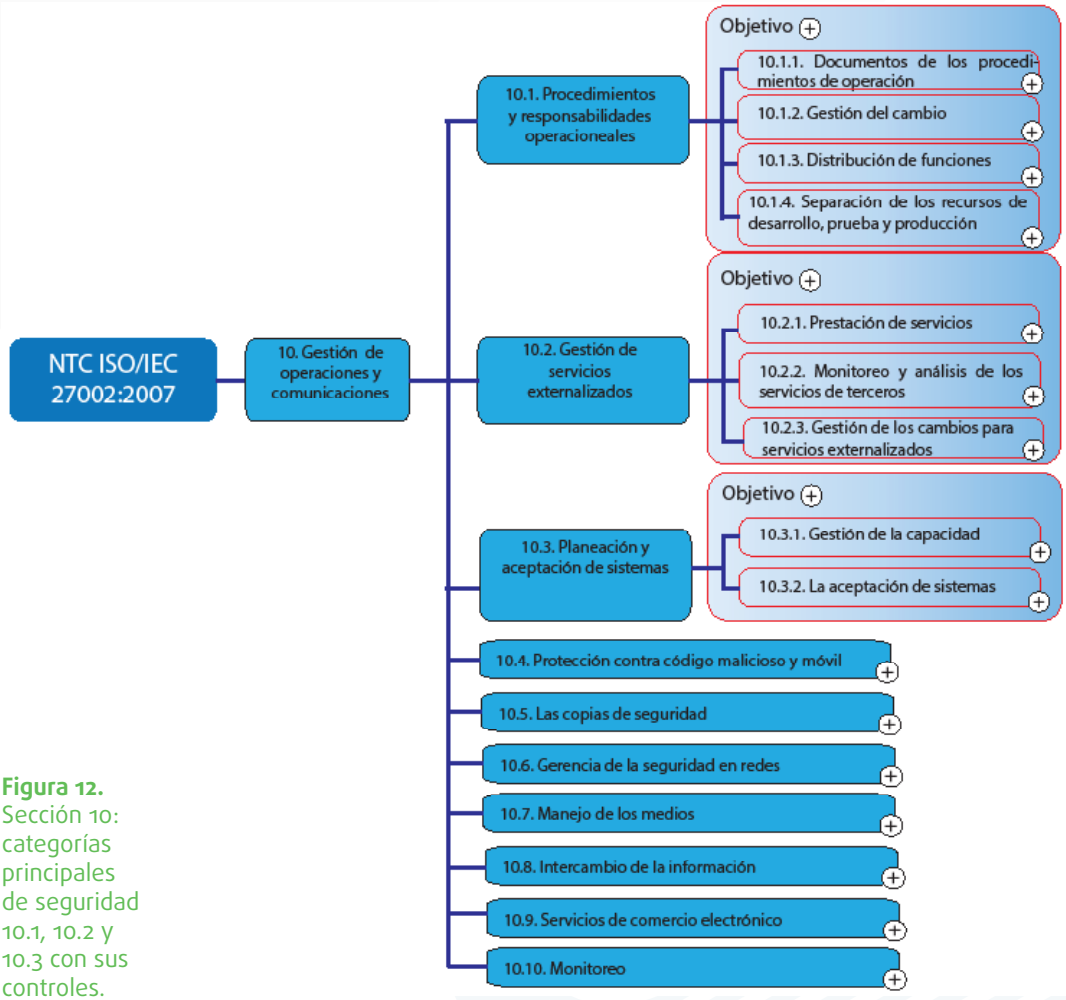


Figura 12. Sección 10: categorías principales de seguridad 10.1, 10.2 y 10.3 con sus controles.

En la categoría 10.1 (procedimientos y responsabilidades operacionales) se muestran los controles que tienen por objeto garantizar el funcionamiento seguro y correcto de los recursos informáticos. En él se describen los controles:

- 10.1.1 (documentos de los procedimientos de operación): se deben aplicar para documentar los procedimientos;
- 10.1.2 (gestión del cambio): define el modo en que se deben controlar las modificaciones y alteraciones;
- 10.1.3 (distribución de funciones): reducción de las oportunidades de uso indebido;

» 10.1.4 (separación de recursos de desarrollo, prueba y producción): describe cómo se deben separar estos ambientes para reducir el riesgo de acceso o modificación no autorizada.

La categoría 10.2 (gestión de servicios externalizados) tiene como objetivo mantener el nivel adecuado de seguridad y de la entrega de servicios de conformidad con los acuerdos. Esta categoría incluye las siguientes medidas de control:

» 10.2.1 (entrega de servicios): se refiere a la garantía de que los controles de seguridad acordados con terceros se cumplan en la realidad;
» 10.2.2 (monitoreo y análisis de los servicios de terceros): aborda la necesidad de seguimiento y análisis crítico que debe hacerse periódicamente;
» 10.2.3 (gestión del cambio para los servicios externalizados): se refiere a la necesidad de gestionar estos servicios de acuerdo al estado crítico de los sistemas y procesos.

En la categoría 10.3 (planeación y aceptación de los sistemas) el objetivo es reducir al mínimo el riesgo de fallas en los sistemas, con la presentación de los dos únicos controles:

» 10.3.1 (gestión de capacidad): se refiere al monitoreo y la sincronización de los recursos con las proyecciones de la capacidad futura para asegurar el rendimiento requerido;
» 10.3.2 (aceptación de sistemas): se refiere a la conveniencia de la realización de pruebas de aceptación de los nuevos sistemas y actualizaciones.

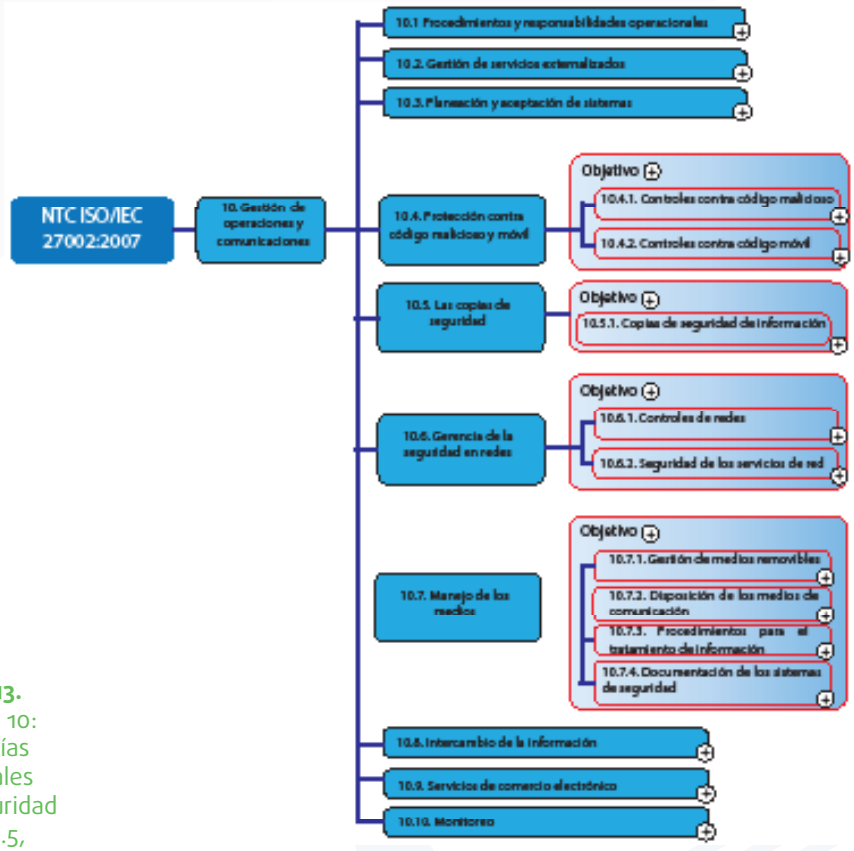


Figura 13. Sección 10: categorías principales de seguridad 10.4, 10.5, 10.6 y 10.7 con sus controles.

La categoría 10.4 (protección contra códigos maliciosos y móviles) tiene por objeto proteger la integridad del software y la información. En esta categoría tenemos a los siguientes controles:

- 10.4.1 (controles contra código malicioso): que describe los procedimientos para la implementación de controles para la detección, prevención y recuperación para protegerse contra código malicioso;
- 10.4.2 (controles contra códigos móviles): muestra las directrices para el uso de código móvil de forma segura.

En la categoría 10.5 (copias de seguridad de información), el objetivo es mantener la integridad y disponibilidad de la información a través del siguiente control:

- 10.5.1 se refiere a la necesidad de que copias de seguridad (*backup*) de la información y de los programas de software sean efectuadas y probadas regularmente.

La categoría 10.6 (gestión de seguridad de la red) tiene por objeto garantizar la protección de la información en las redes y la protección de la infraestructura de soporte. Esta categoría tiene dos controles:

- 10.6.1 (control de redes): se refiere a la necesidad de una adecuada gestión y control de las redes, incluida la información en tránsito;
- 10.6.2 (seguridad de los servicios de red): describe la necesidad de que los niveles de los servicios de red sean identificados e incluidos en los acuerdos de nivel de servicio.

En la categoría 10.7 (manipulación de medios) se describen los controles que deben ser aplicados para evitar la divulgación no autorizada, modificación, supresión o destrucción. Son los siguientes controles:

- 10.7.1 (gestión de medios removibles): describe la necesidad de controles para la gestión de medios removibles;
- 10.7.2 (eliminación de medios): muestra cómo se debe realizar la eliminación de los medios;
- 10.7.3 (procedimientos para el manejo de la información): presenta los controles que deben ser aplicados para el manejo y almacenamiento de la información, evitando la divulgación no autorizada;
- 10.7.4 (seguridad de la documentación del sistema): presenta el control de protección de la documentación del sistema.

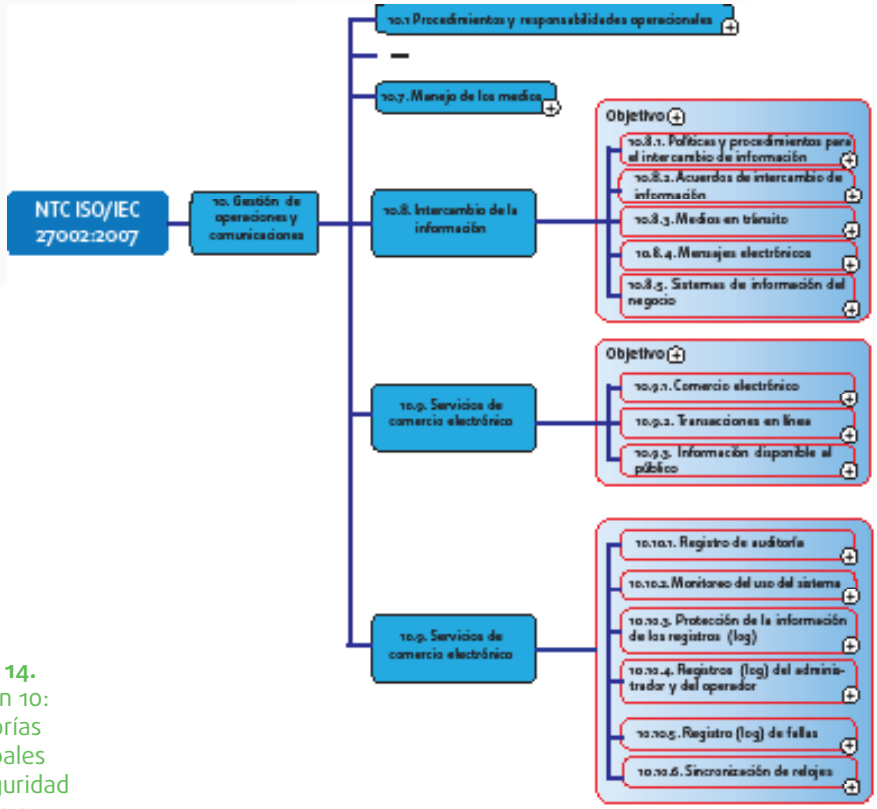


Figura 14. Sección 10: categorías principales de seguridad 10.8, 10.9, y 10.10 con sus controles.

La categoría 10.8 (intercambio de información) tiene como objetivo mantener la seguridad en el intercambio de la información interna y con entidades externas. Posee los siguientes controles:

- 10.8.1 (políticas y procedimientos para el intercambio de información): es conveniente que sean establecidas políticas y procedimientos para proteger el intercambio de información;
- 10.8.2 (acuerdos de intercambio de información): se deben establecer acuerdos para el intercambio de información;
- 10.8.3 (medios en tránsito): es recomendable que el transporte de los medios se haga bajo protección contra el uso indebido o el acceso no autorizado de esos dichos medios;

- 10.8.4 (mensajes electrónicos): es conveniente que los mensajes estén protegidos adecuadamente;
- 10.8.5 (sistema de información del negocio): se recomienda que las políticas y procedimientos estén diseñados para proteger la información en las interconexiones del sistema.

En la categoría 10.9 (servicios de comercio electrónico), el objetivo es garantizar la seguridad durante el uso de los servicios de comercio electrónico y su uso seguro. En esta categoría se encuentran los controles:

- 10.9.1 (comercio electrónico): se refiere a la protección de la información involucrada en el comercio electrónico contra las actividades fraudulentas;
- 10.9.2 (transacciones en línea): conviene realizar la protección de información para prevenir la transmisión incompleta, entre otros;
- 10.9.3 (información disponible al público): es recomendable asegurar la integridad de la información proporcionada en los sistemas públicos.

La categoría 10.10 (monitoreo) tiene como objetivo detectar las actividades no autorizadas de procesamiento de información. Los controles son:

- 10.10.1 (registros de auditoría): es importante que todos los *log* de auditoría de eventos de seguridad se generen y se conserven durante un período de tiempo acordado;
- 10.10.2 (monitoreo del uso del sistema): se deben establecer procedimientos para supervisar el uso de los recursos de procesamiento de la información;
- 10.10.3 (protección de la información de los registros (*log*)): los logs deben estar protegidos contra cambios no autorizados y problemas operacionales;
- 10.10.4 (registros (*log*) de administrador y operador): se recomienda registrar las actividades de los administradores y operadores del sistema;
- 10.10.5 (registros (*logs*) de las fallas): es conveniente que las fallas sean registradas y analizadas;
- 10.10.6 (sincronización de relojes): todos los sistemas relevantes deben tener sus relojes sincronizados.

Ejercicio de refuerzo - sección 10: gestión de operaciones y comunicaciones

Utilizando la norma, explique los controles

- 10.1.3
- 10.2.2
- 10.4.1
- 10.5.1
- 10.6.2
- 10.7.1
- 10.10.2

2.9 Sección 11: control de acceso

En la sección 11 (control de acceso) se encuentran las categorías que abordan los controles necesarios a los controles de acceso lógico. A diferencia de la sección 9 (seguridad física y del ambiente), en la sección 11 se abordarán aspectos relacionados con los privilegios de acceso, contraseñas, acceso a la red, entre otros. En esta sección hay siete principales categorías de seguridad.

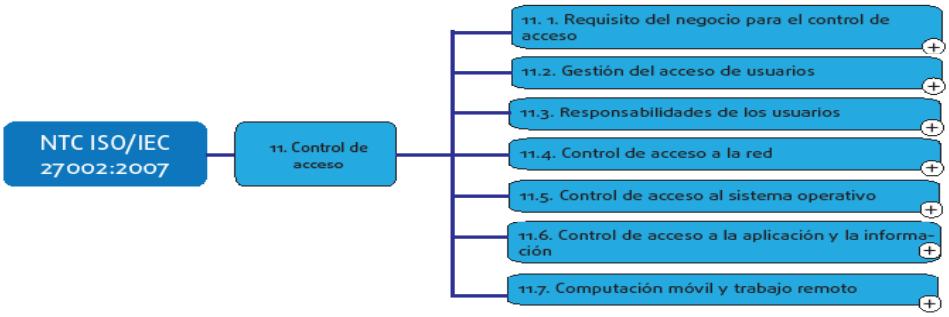


Figura 15. Sección 11 y sus siete categorías principales de seguridad

En la siguiente figura se establecen las principales categorías de seguridad y sus respectivos controles: categoría 11.1 (requisitos de negocio para el control de acceso), categoría 11.2 (gestión de acceso de usuario) y categoría 11.3 (responsabilidades de los usuarios).

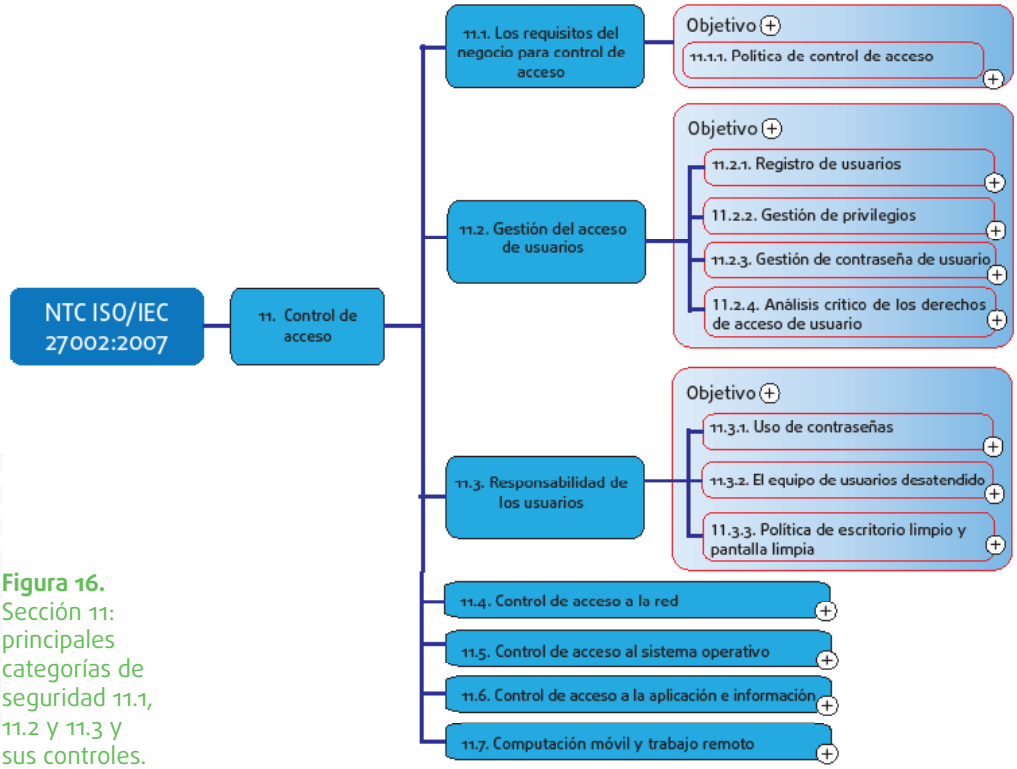


Figura 16. Sección 11: principales categorías de seguridad 11.1, 11.2 y 11.3 y sus controles.

En la categoría 11.1 (requisitos de negocio para el control de acceso) el objetivo es controlar el acceso a la información. El control es:

» 11.1.1 (política de control de acceso): debe haber una política de control de acceso establecida y analizada críticamente.

La categoría 11.2 (gestión de acceso de usuario): tiene como objetivo garantizar el acceso a los usuarios autorizados y evitar el acceso no autorizado. Los controles son:

- 11.2.1 (registro de usuario): describe la conveniencia de la existencia de un procedimiento formal de registro y cancelación de usuarios;
- 11.2.2 (gestión de privilegios): muestra la necesidad de que la concesión y uso de privilegios deben ser restringidos y controlados;
- 11.2.3 (gestión de contraseña): tiene la ventaja de que la concesión de las contraseñas sea controlada;
- 11.2.4 (análisis crítico de los derechos de acceso de usuario): presenta la conveniencia de que el administrador realice análisis críticos periódicos sobre los derechos de acceso de los usuarios.

La categoría 11.3 (responsabilidades de los usuarios) tiene por objeto prevenir el acceso no autorizado y evitar la afectación o el robo de los recursos. Contamos con los controles:

- 11.3.1 (uso de contraseñas): aborda la necesidad de los usuarios a seguir las mejores prácticas en el uso y la selección de las contraseñas;
- 11.3.2 (equipo del usuario desatendido): muestra la importancia de que los equipos desatendidos tengan la protección adecuada;
- 11.3.3 (política de escritorio limpio y pantalla limpia): muestra la conveniencia de adoptar una política de mesa limpia de papeles y de medios, y también de pantalla limpia.

En la siguiente figura se establecen las principales categorías de seguridad y sus respectivos controles: categoría 11.4 (control de acceso a redes) y categoría 11.5 (control de acceso al sistema operativo).

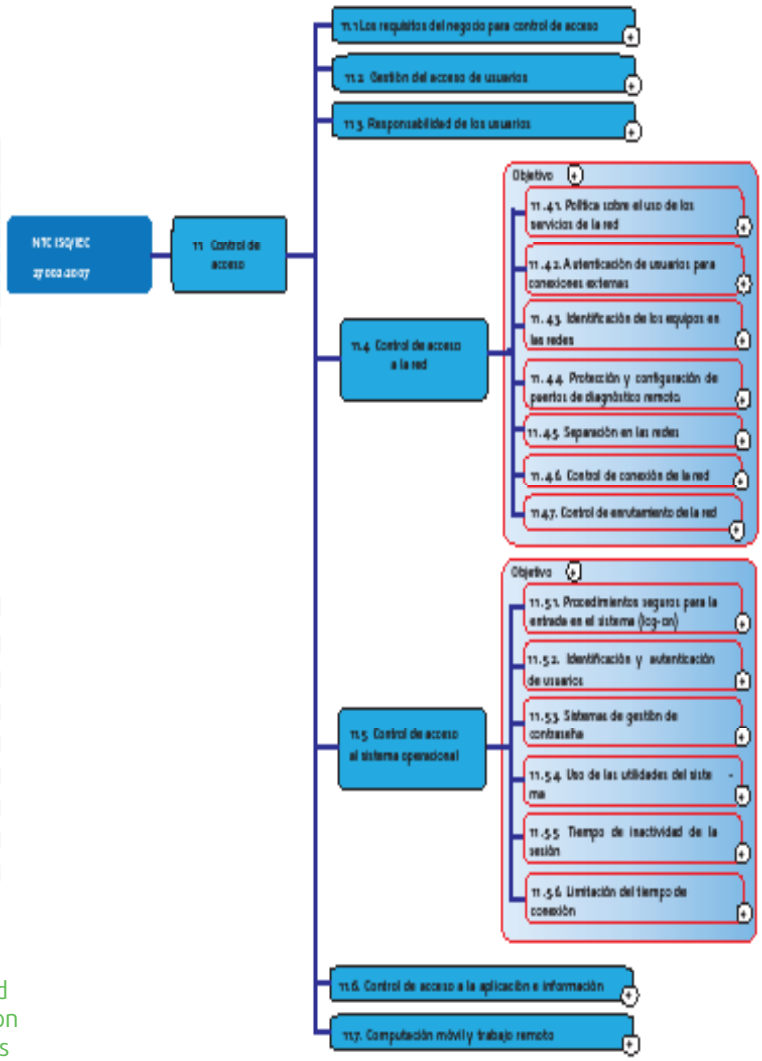


Figura 17. Sección 11: categorías principales de seguridad 11.4 y 11.5 con sus controles

La categoría 11.4 (control de acceso a redes) tiene por objeto prevenir el acceso no autorizado a los servicios de red. Tiene los siguientes controles:

- 11.4.1 (política de uso de los servicios de red): presenta la conveniencia de que los usuarios reciban acceso sólo a los servicios que hayan sido autorizados a usar;
- 11.4.2 (autenticación de usuarios para conexiones externas): recomienda que se usen métodos adecuados para controlar el acceso de usuarios remotos;

- 11.4.3 (identificación de los equipos en las redes): recomienda la conveniencia de permitir la identificación automática de los equipos;
- 11.4.4 (protección y configuración de puertos de diagnóstico remoto): recomienda que se controle el acceso físico y lógico a los puertos de diagnóstico y configuración;
- 11.4.5 (separación en las redes): recomienda que los usuarios y los sistemas sean separados en las redes;
- 11.4.6 (control de conexión de red): recomienda que la capacidad de los usuarios para conectarse a la red esté restringida,
- 11.4.7 (control de enrutamiento de la red): presenta la recomendación de que se implemente un control de enrutamiento de red para que las conexiones de red y los flujos de información no violen la política de control de acceso.

La categoría 11.5 (control de acceso al sistema operativo) tiene por objeto prevenir el acceso no autorizado a los sistemas operativos. Los controles son:

- 11.5.1 [Los procedimientos seguros para la entrada al sistema (*log-on*)]: muestra la conveniencia de que el acceso sea controlado por un procedimiento seguro para la entrada en el sistema;
- 11.5.2 (identificación y autenticación de usuarios): presenta la conveniencia de que todos los usuarios tengan un identificador único, con una técnica adecuada para la validación de la identidad del usuario;
- 11.5.3 (sistema de gestión de contraseñas): recomienda que los sistemas para la gestión de las contraseñas sean interactivos;
- 11.5.4 (uso de las utilidades del sistema): recomienda que el uso de las utilidades del sistema sea restringido y controlado;
- 11.5.5 (tiempo de inactividad de la sesión): muestra la necesidad de suspender las sesiones inactivas;
- 11.5.6 (limitación del tiempo de conexión): presenta la posibilidad de realizar restricciones en los tiempos de conexión.

En la siguiente figura se establecen las principales categorías de seguridad y sus respectivos controles: categoría 11.6 (control de acceso a las aplicaciones y la información) y categoría 11.7 (computación móvil y trabajo remoto).

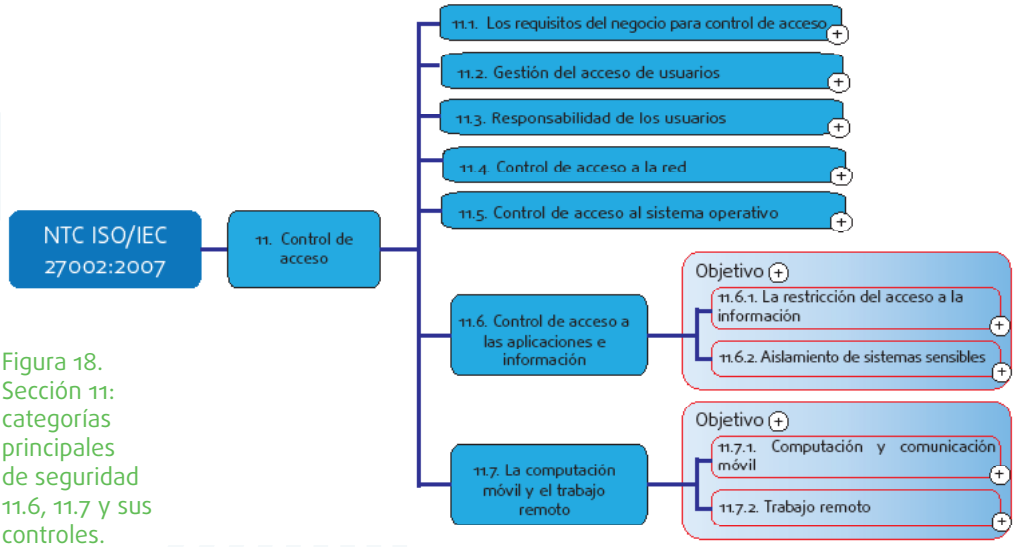


Figura 18. Sección 11: categorías principales de seguridad 11.6, 11.7 y sus controles.

En la categoría 11.6 (control de acceso a las aplicaciones y a la información), el objetivo es prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación. Los controles son:

- 11.6.1 (restricción de acceso a la información): establece que el acceso a la información y las funciones de los sistemas de aplicación de los usuarios y personal de soporte sean restringidos;
- 11.6.2 (aislamiento de sistemas sensibles): recomienda que los sistemas sensibles tengan un ambiente informático aislado.

La categoría 11.7 (computación móvil y trabajo remoto) tiene como objetivo garantizar la seguridad de la información cuando se utilizan la computación móvil y el trabajo remoto. Los controles son:

- 11.7.1 (computación y comunicación móvil): recomienda la adopción de políticas y medidas contra los riesgos debidos al uso de los recursos informáticos y de comunicaciones móviles;
- 11.7.2 (trabajo remoto): presenta las ventajas de que las políticas, planes y procedimientos sean elaborados e implementados para el trabajo remoto.

Ejercicio de refuerzo - sección 11: control de acceso

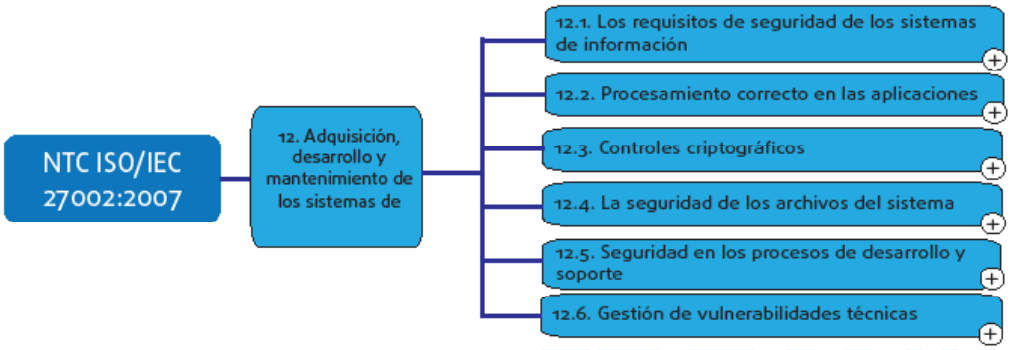
Utilizando la norma, explique los controles

- 11.1.1
- 11.2.2
- 11.3.3
- 11.5.5
- 11.6.2

2.10 Sección 12: adquisición, desarrollo y mantenimiento de sistemas de información.

En la sección 12 (adquisición, desarrollo y mantenimiento de sistemas de información) están los controles sobre la adquisición, desarrollo y mantenimiento de las actividades de software. El objetivo de esta sección es desarrollar la seguridad de la información en las aplicaciones de la organización. Esta sección tiene seis categorías principales de seguridad.

Figura 19. Sección 12 y sus seis categorías principales de seguridad



En la siguiente figura se establecen las principales categorías de seguridad y sus respectivos controles: categoría 12.1 (requisitos de seguridad de sistemas de información), categoría 12.2 (procesamiento correcto en las aplicaciones) y categoría 12.3 (controles criptográficos).

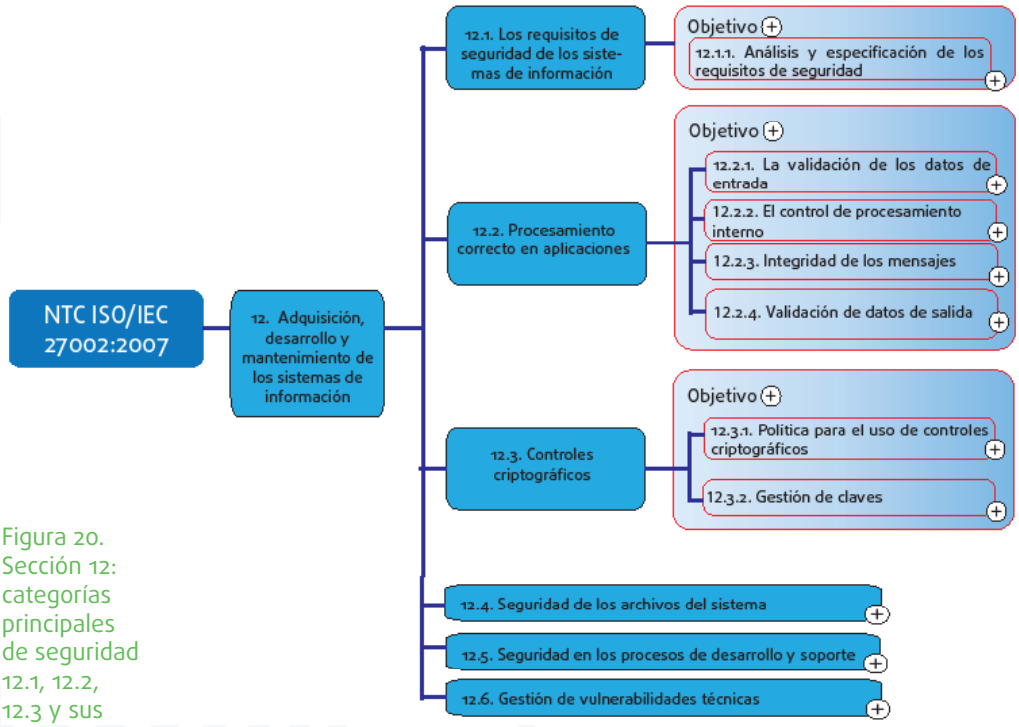


Figura 20. Sección 12: categorías principales de seguridad 12.1, 12.2, 12.3 y sus controles.

La categoría 12.1 (requisitos de seguridad de sistemas de información) tiene por objeto garantizar que la seguridad es una parte integrante de los sistemas de información. Tiene el siguiente control:

» 12.1.1 (análisis y especificación de requisitos de seguridad): define los controles de seguridad en las especificaciones de requisitos para los nuevos sistemas.

En la categoría 12.2 (procesamiento correcto en las aplicaciones) el objetivo es prevenir la ocurrencia de errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Los controles son:

» 12.2.1 (validación de datos de entrada): establece que los datos de entrada a las aplicaciones sean validados para asegurar que son correctos y adecuados;
» 12.2.2 (control de procesamiento interno): se recomienda comprobar que la validación se incorpora en las aplicaciones para detectar corrupción de datos;

- 12.2.3 (integridad de mensajes): establece que se implementen requisitos para garantizar la autenticidad y proteger la integridad;
- 12.2.4 (Validación de datos de salida): se recomienda que los datos de salida sean validados para garantizar que el procesamiento es correcto.

La categoría 12.3 (controles criptográficos) tiene por objeto proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos. Los controles son:

- 12.3.1 (política sobre el uso de controles criptográficos): en ella se recomienda que se desarrolle e implemente una política para el uso de controles criptográficos.
- 12.3.2 (gestión de claves): presenta las ventajas de que un proceso de gestión de claves sea implantado para apoyar el uso de técnicas criptográficas

En la siguiente figura se establecen las principales categorías de seguridad y sus respectivos controles: categoría 12.4 (seguridad de los archivos del sistema), categoría 12.5 (seguridad en los procesos de desarrollo y soporte) y categoría 12.6 (gestión de las vulnerabilidades técnicas).

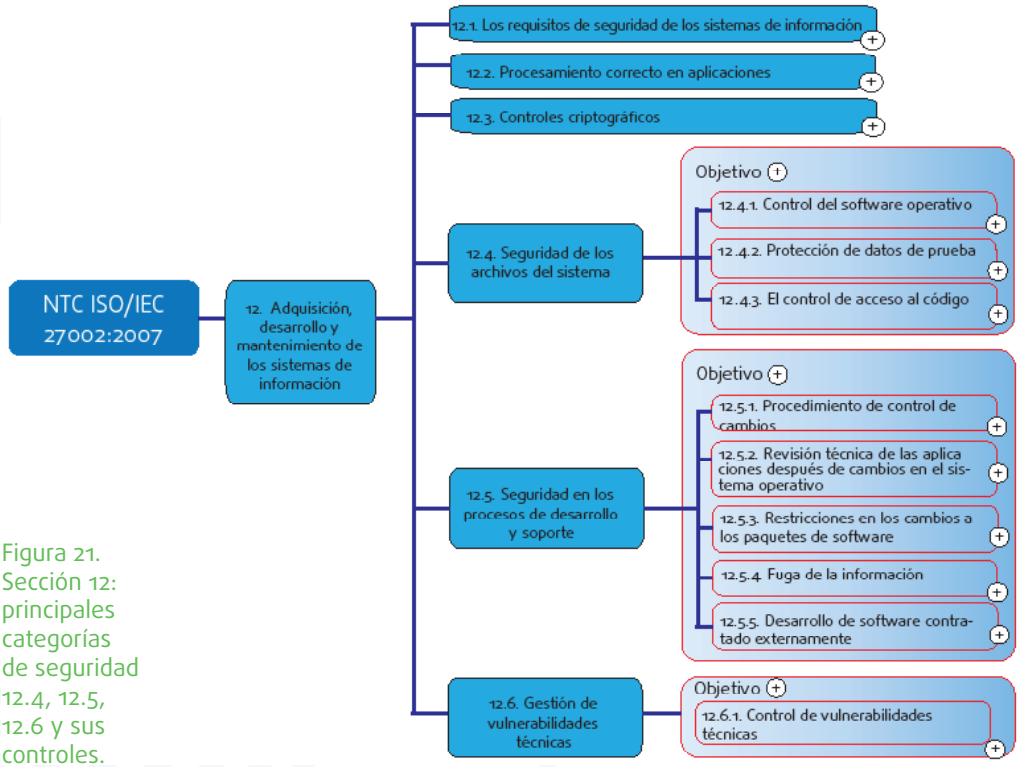


Figura 21. Sección 12: principales categorías de seguridad 12.4, 12.5, 12.6 y sus controles.

La categoría 12.4 (seguridad de los archivos del sistema) tiene por objeto garantizar la seguridad de los archivos del sistema. Los controles son:

- 12.4.1 (control de software operativo): se deben implementar procedimientos para el control de la instalación de software en los sistemas operativos;
- 12.4.2 (protección de datos para la prueba del sistema): presenta la recomendación de que los datos de prueba sean seleccionados con cuidado, protegidos y controlados,
- 12.4.3 (controlar el acceso al código fuente del programa): especifica que el acceso al código fuente sea restringido.

La categoría 12.5 (seguridad en los procesos de desarrollo y soporte) tiene como objetivo mantener la seguridad de los sistemas de información y aplicaciones. Posee los controles:

- 12.5.1 (procedimientos de control de cambios): es conveniente que la implementación de cambios sea controlada con el uso de procedimientos formales de control de cambios;

- 12.5.2 (revisión técnica de las aplicaciones después de los cambios del sistema operativo): considera conveniente que las aplicaciones críticas sean analizadas y probadas cuando se cambian los sistemas operativos;
- 12.5.3 (restricciones a los cambios en los paquetes de software): presenta la recomendación de que todos los cambios sean estrictamente controlados;
- 12.5.4 (fuga de información): resalta la necesidad de evitar toda oportunidad de fuga de información;
- 12.5.5 (desarrollo de software contratado externamente): la organización debe supervisar y monitorear el desarrollo de software contratado externamente.

En la categoría 12.6 (gestión de las vulnerabilidades técnicas) el objetivo es reducir los riesgos derivados de la explotación de las vulnerabilidades técnicas conocidas. El control es:

- 12.6.1 (control de las vulnerabilidades técnicas): es conveniente obtener información sobre las vulnerabilidades técnicas, los riesgos deben ser evaluados y se deben tomar los cuidados necesarios.

Ejercicio de refuerzo - sección 12: adquisición, desarrollo y mantenimiento de sistemas de información.

Utilizando la norma, explique los controles

- 12.1.1
- 12.2.2
- 12.3.1
- 12.5.4
- 12.6.1

2.11 Sección 13: gestión de incidentes de seguridad de la información.

Sección 13 (gestión de incidentes de seguridad de la información) se refiere al reporte de eventos de seguridad, las responsabilidades y el proceso de recolección de evidencia. Tiene dos categorías de seguridad principales.

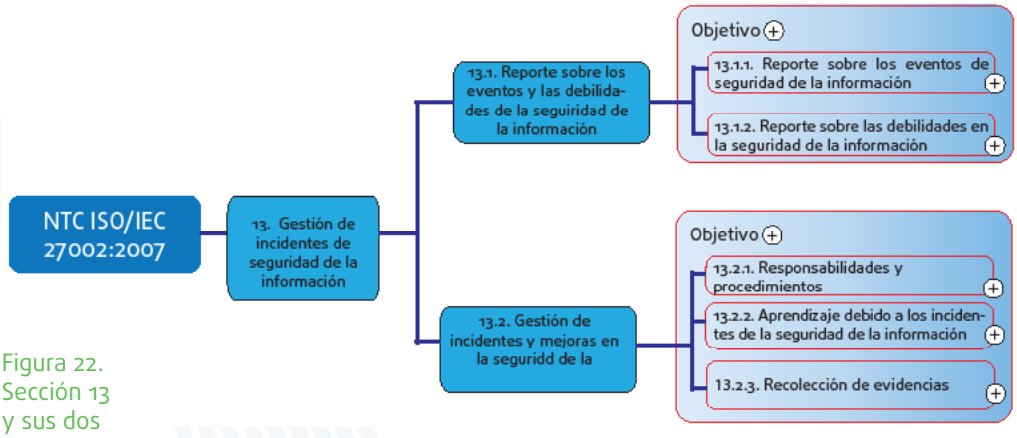


Figura 22. Sección 13 y sus dos principales categorías de seguridad y los controles

La categoría 13.1 (reportes sobre los eventos y las debilidades de la seguridad de la información) tiene como objetivo asegurar que los eventos y las debilidades de la seguridad sean comunicados, permitiendo tomar medidas correctivas en tiempo real. Tiene los controles:

- 13.1.1 (reporte sobre los eventos de seguridad de la información): define que los eventos de seguridad sean informados a través de los canales apropiados tan pronto como sea posible,
- 13.1.2 (reporte sobre las debilidades en la seguridad de la información): se recomienda que todos los recursos humanos sean instruidos para registrar y reportar cualquier observación o sospecha de deficiencia de los sistemas y servicios.

La categoría 13.2 (gestión de incidentes y mejoras en la seguridad de la información) tiene por objeto garantizar que un enfoque coherente y eficaz sea aplicado a la gestión de incidentes de seguridad de la información. Los controles son:

- 13.2.1 (responsabilidades y procedimientos): presenta la conveniencia de que las responsabilidades y los procedimientos se establezcan para garantizar una respuesta rápida;
- 13.2.2 (aprendizaje debido a los incidentes de seguridad de la información): recomienda que se establezcan mecanismos para monitorear y cuantificar los tipos y costos de los incidentes;

» 13.2.3 (recolección de evidencia): presenta la necesidad de recolectar la evidencia, almacenarla y se presentarla de conformidad con la legislación pertinente.

Ejercicio de refuerzo - sección 13: gestión de incidentes de seguridad de la información.

Utilizando la norma, explique los controles

» 13.1.1
» 13.1.2
» 13.2

2.12 Sección 14: gestión de la continuidad del negocio.

La sección 14 (gestión de la continuidad del negocio) se encarga de todos los aspectos de la continuidad en el caso de un desastre. Esta sección tiene una sola categoría principal de seguridad.

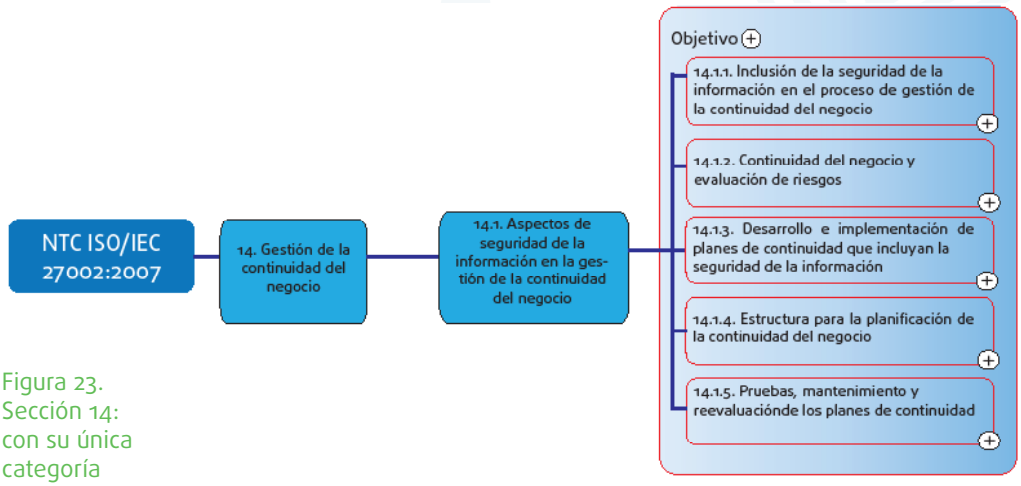


Figura 23. Sección 14: con su única categoría principal de la seguridad y sus controles

La categoría 14.1 (aspectos de seguridad de la información en la gestión de la continuidad del negocio) tiene como objetivo no permitir la interrupción de las actividades del negocio y proteger los procesos críticos contra los efectos de fallas o desastres significativos, y asegurar su reactivación de manera oportuna, si es el caso. Los controles son:

- 14.1.1 (inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio): es conveniente que sea desarrollado y mantenido un proceso de gestión de continuidad de negocio de la organización, contemplando los requisitos de seguridad;
- 14.1.2 (continuidad del negocio y evaluación de riesgos): se deben identificar los eventos que pueden causar la interrupción del negocio;
- 14.1.3 (desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información): es importante que los planes se elaboren y se implementen;
- 14.1.4 (estructura para la planificación para la continuidad del negocio): presenta la necesidad de una estructura básica y consistente de los planes de continuidad del negocio;
- 14.1.5 (pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio): los planes deben ser probados y actualizados con regularidad.

Ejercicio de refuerzo - sección 14: gestión de la continuidad del negocio

Utilizando la norma, explique los controles

- 14.1.2
- 14.1.3

2.13 Sección 15: cumplimiento

La sección 15 (cumplimiento) establece que los requisitos de seguridad de la información estén de acuerdo con cualquier Ley (legalidad), como reglamentos, estatutos u obligaciones contractuales. Esta sección tiene tres categorías principales de seguridad.

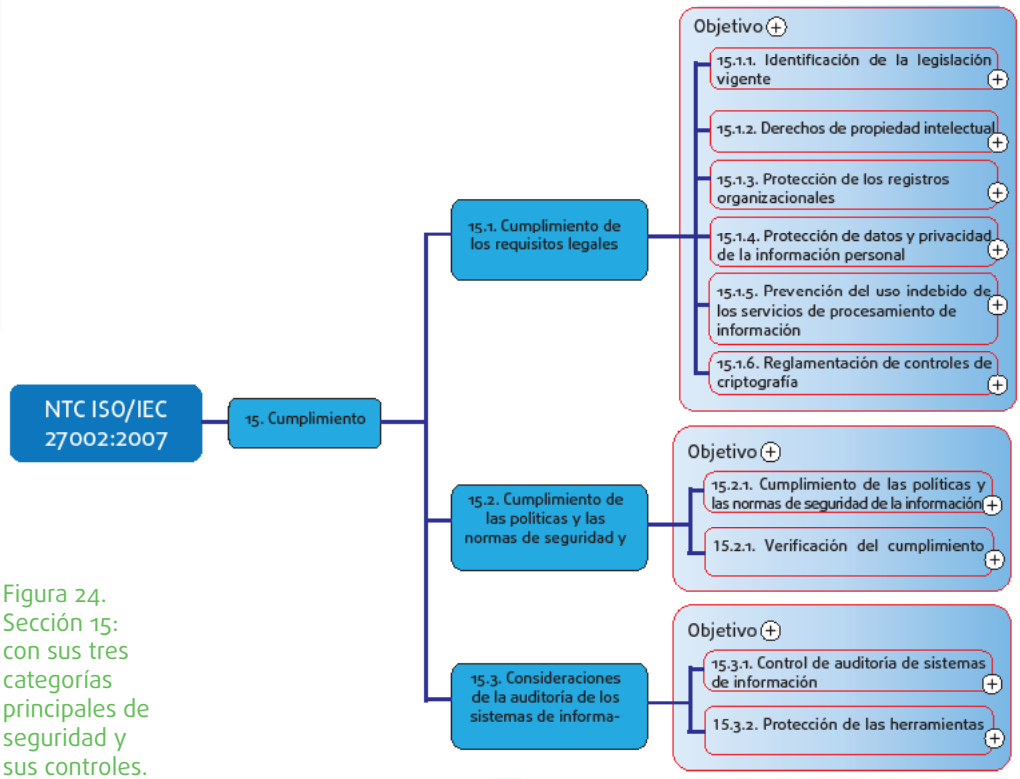


Figura 24. Sección 15: con sus tres categorías principales de seguridad y sus controles.

La categoría 15.1 (cumplimiento de los requisitos legales) tiene como objetivo prevenir la violación de cualquier Ley penal o civil, estatutos, reglamentaciones u obligaciones contractuales y cualquier otro requisito de seguridad de la información. Cuenta con los siguientes controles:

- 15.1.1 (identificación de la legislación vigente): considera conveniente que todos los requisitos legales y contractuales se definan explícitamente, y sean documentados y mantenidos;
- 15.1.2 (derechos de propiedad intelectual): recomienda que se implementen procedimientos para garantizar el cumplimiento de los derechos de propiedad intelectual;
- 15.1.3 (protección de los registros organizacionales): recomienda que los registros sean protegidos contra pérdida, destrucción y falsificación;
- 15.1.4 (protección de datos y privacidad de la información personal): indica que la privacidad y la protección de datos sean garantizadas;
- 15.1.5 (prevención del uso indebido de los servicios de procesa-

miento de información): se recomienda que los usuarios sean disuadidos de usar los servicios informáticos para propósitos no autorizados,
» 15.1.6 (Reglamento de controles criptográficos): recomienda que controles criptográficos se utilicen de acuerdo con la legislación vigente.

La categoría 15.2 (cumplimiento de las normas y políticas para la seguridad de la información y cumplimiento técnico) tiene por objeto garantizar la conformidad de los sistemas con las políticas y normas organizacionales de seguridad de la información. Sus controles son:

» 15.2.1 (cumplimiento con las políticas y normas de seguridad de la información): recomienda que los gestores garanticen que todos los procedimientos de seguridad de la información dentro de su área están funcionando correctamente,
» 15.2.2 (verificación del cumplimiento técnico): considera conveniente que los sistemas de información sean verificados periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.

En la categoría 15.3 (consideraciones de la auditoría de los sistemas de información), el objetivo es maximizar la eficacia y minimizar la interferencia en el proceso de auditoría de los sistemas de información. Los controles son:

» 15.3.1 (controles de auditoría de sistemas de información): los requisitos y las actividades de auditoría deben ser cuidadosamente planificados.
» 15.3.2 (protección de las herramientas de auditoría de sistemas de información): se debe proteger el acceso a las herramientas de auditoría de los sistemas de información.

Ejercicio de refuerzo - sección 15: cumplimiento

Utilizando la norma, explique los controles

» 15.1.1
» 15.1.2
» 15.1.4
» 15.2.1
» 15.3.1

Capítulo

03

Sistema de gestión de seguridad de la información

Objetivos

Presentar una visión general y el alcance del Sistema de Gestión de Seguridad de la Información, SGSI, así como un análisis crítico y detallado de los controles. También se presentará el modelo Planear, Hacer, Verificar, Actuar, PHVA.

Conceptos

Modelos SGSI y PHVA.

3.1 Visión general y alcance

El modelo del SGSI integra la estrategia de la organización y está influenciada por factores tales como:

- Necesidades y objetivos.
- Requisitos de seguridad.
- Procesos.
- Estructura organizacional.

La norma ISO/IEC 27001:2005 fue preparada para ofrecer un modelo para establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar un SGSI.

Ejercicio de nivelación – SGSI

- ¿Qué entiende usted por gestión?
- ¿Qué entiende usted por sistema de gestión?

La adopción de un SGSI debe ser una decisión estratégica para la organización. La especificación y la implementación del SGSI de una organización están influenciadas por sus necesidades y objetivos, requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Se espera que la implementación de un SGSI sea proporcional de acuerdo con las necesidades de la organización; por ejemplo, una situación simple requiere una solución de un SGSI sencillo.

3.2 Modelo PHVA

La norma ISO 27001 adopta el modelo conocido como PHVA, que se aplica para estructurar todos los procesos del SGSI.

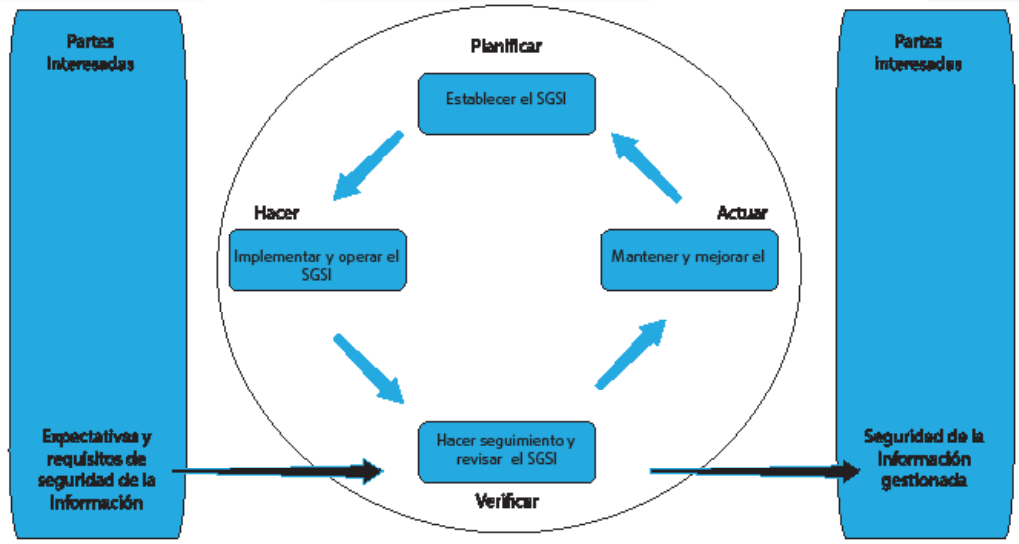


Figura 25.
Modelo PHVA

El modelo PHVA comprende un conjunto de acciones en la secuencia establecida por las letras que componen las siglas: P (plan: planear), H (hacer, ejecutar), V (verificar, controlar) y, finalmente, A (actuar, actuar de manera correctiva):

- **Planear** (establecer el SGSI): establecer las políticas, objetivos, procesos y procedimientos del SGSI, relevantes para la gestión del riesgo y la mejora de la seguridad de información, para conseguir resultados de acuerdo con las políticas y objetivos generales de una organización.
- **Hacer** (implementar y operar el SGSI): implementar y operar las políticas, controles, procesos y procedimientos del SGSI.
- **Verificar** (comprobar: monitorear y analizar críticamente el SGSI): evaluar y, si es el caso, medir el desempeño de un proceso con base en la política, los objetivos y la experiencia práctica del SGSI y presentar los resultados para la revisión de la dirección.

» **Actuar** (mantener y mejorar el SGSI): llevar a cabo las acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y el análisis crítico realizado por la dirección u otra información pertinente, para lograr la mejora continua del SGSI.

ISO/IEC 27002:2007 (Tecnología de la Información: Técnicas de Seguridad): código de práctica para la gestión de seguridad de la información. Los términos y definiciones dados en la Norma ISO/IEC 27002 son válidos y aplicables para resolver dudas.

Ejercicio de refuerzo - modelo PHVA

» Explique el modelo PHVA.
» Explique cómo el modelo PHVA se aplica a los SGSI. Utilice la norma para fundamentar su respuesta.

3.3 Sistema de Gestión de la Seguridad de la Información, SGSI

El SGSI en inglés *Information Security Management System*, ISMS, es un proceso estructurado de tratamiento de seguridad de la información en los diversos sectores. Ahora vamos a ver sus puntos principales para una implementación perfecta.

Para los propósitos de esta norma, el proceso utilizado se basa en el modelo PHVA. Su requisito general presenta cómo debe, la organización, obligatoriamente, tratar el proceso SGSI. Los siete verbos de acción indican cada fase o etapa del ciclo de vida del SGSI.

3.4 Estableciendo y gerenciando el SGSI

A continuación se presenta cada etapa en la gestión de un SGSI:

» Establecer el SGSI.
» Implementar y operar el SGSI.
» Monitorear y analizar críticamente el SGSI.
» Mantener y mejorar el SGSI.

3.4.1 Establecer el SGSI

Los siguientes requisitos se deben cumplir dentro de cualquier organización, al iniciar un proceso de establecimiento de un SGSI:

- **Definir el alcance:** debe considerar las características del negocio, la organización, la ubicación, los activos y la tecnología;
- **Definir la política de seguridad:** además de obedecer al alcance, debe fijar objetivos y establecer la dirección general para las acciones relacionadas con la seguridad. Tendrá en cuenta los requisitos legales, reglamentarios, contractuales y de negocios. La política de seguridad debe estar alineada con el contexto de la gestión del riesgo en la organización, y establecer criterios para la evaluación y ser aprobado por la dirección;
- **Definir la estrategia de evaluación de riesgos:** determinar la metodología y desarrollar criterios para la aceptación;
- **Hacer la identificación, análisis y evaluación de riesgos:** identificar los activos, vulnerabilidades y amenazas. Evaluar posibles daños, estimar la probabilidad y calcular el riesgo, determinando si éste es aceptable o requiere tratamiento;
- **Identificar y evaluar las opciones para el tratamiento de los riesgos:** implementar controles, aceptar, evitar, transferir el riesgo;
- **Seleccionar los controles y los objetivos para el tratamiento del riesgo:** seleccione los controles de la norma que han de aplicarse;
- **Obtener aprobación para los riesgos residuales;**
- **Obtener el consentimiento para la implementación del SGSI;**
- **Preparar la declaración de aplicabilidad:** debe relacionar los objetivos de control y los controles seleccionados, justificando obligatoriamente aquellos no seleccionados.

Ejercicio de refuerzo - establecer el SGSI

Lea los artículos 4.2.1 y 4.2.2 de la norma NTC ISO/IEC 27001:2005.

- Explique el requisito de definir la política de seguridad en el establecimiento de un SGSI. Utilice la norma 27001.

3.4.2 Implementación y operación del SGSI

Cumplidos los requisitos necesarios para establecer el SGSI, se debe analizar, para el ambiente de la organización, la forma de cumplir los requisitos de implementación y operación:

- **Formular e implementar el tratamiento del riesgo:** como resultado del análisis de riesgos, la organización debe implementar un plan de tratamiento de riesgos eficiente;
- **Implementar los controles seleccionados:** a partir de los controles identificados como necesarios para el tratamiento de los riesgos de la organización deben implementarlos;
- **Definir parámetros para medir la eficacia de los controles:** desarrollar parámetros de medición, métricas e indicadores para evaluar la eficiencia y eficacia de los controles;
- **Implementar un programa de entrenamiento:** poseer y poner en práctica un programa de capacitación eficaz es esencial para el éxito;
- **Gestionar las operaciones del SGSI:** saber cómo está funcionando el SGSI y buscar áreas de mejora;
- **Gestionar los recursos para el SGSI:** comprobar si los recursos son suficientes;
- **Implementar controles capaces de detectar y responder a los incidentes de seguridad:** crear mecanismos de respuesta a cualquier incidente de seguridad de forma inmediata y planificada.

Ejercicio de refuerzo - implementación y operación del SGSI

- Cite dos requisitos de implementación y operación

3.4.3 Monitoreo y análisis crítico del SGSI

Esenciales en cualquier sistema de gestión, las actividades de monitoreo y revisión son fundamentales para el éxito de un SGSI, al permitir el seguimiento, a través de evidencias, así como el proceso de mejoramiento continuo del sistema. Así tenemos, para esta fase, los siguientes requisitos:

- **Ejecutar los procedimientos de monitoreo y análisis crítico:** detectar los errores en el procesamiento, identificar inmediatamente las fallas, brechas de seguridad e incidentes, y controlar si se llevan a cabo las actividades delegadas como fue especificado, en caso de una falla de seguridad;
- **Llevar a cabo revisiones periódicas de la eficacia del SGSI;**
- **Revisar el riesgo:** considerar los cambios relacionados con la organización, la tecnología, los objetivos y los procesos de negocio, las amenazas identificadas, eventos externos, tales como contratos, la legislación y el contexto social;
- **Actualizar el plan de seguridad;**
- **Mantenga registro de las acciones y eventos que han impactado sobre la eficacia o el rendimiento del SGSI.**

3.4.4 Mantenimiento y mejora del SGSI

Esta fase tiene como objetivo presentar los requisitos que la organización, de forma regular y estructurada, debe cumplir para que su SGSI se mantenga dentro del proceso de mejoramiento continuo del PHVA. Es interesante señalar la importancia de las acciones preventivas para este caso:

- **Implementar las mejoras identificadas:** las acciones necesarias se han identificado en la fase anterior;
- **Ejecutar las acciones preventivas y correctivas:** es necesario realizar acciones que puedan anticipar posibles ocurrencias;
- **Comunicar las acciones y mejoras:** Comunicar a todos los involucrados los cambios realizados en el SGSI;
- **Asegurar que las mejoras alcancen sus objetivos:** crear mecanismos para comprobar que se están cumpliendo los objetivos.

Ejercicio de refuerzo - mantenimiento y mejora del SGSI

Lea los artículos 4.2.3 y 4.2.4 de la norma NTC ISO/IEC 27001:2005.

- ¿Por qué es importante esta etapa? Utilice la norma 27001 para responder.

3.5 Requisitos generales de la documentación

La documentación dentro de un SGSI es un importante factor de éxito, dado que demuestra la relación de los resultados esperados con los controles implementados. La documentación será a menudo la evidencia necesaria para averiguar que un SGSI está implementado de manera correcta y eficiente, permitiendo que las acciones puedan ser trazables y reproducibles.

Declaración de aplicabilidad:

Es un documento formal que contiene los controles aplicados, los controles no aplicados, los controles no aplicables y los controles adicionales. Se trata de una lista de todos los controles de la norma indicando: los controles aplicados y el riesgo que se está tratando, los controles no aplicados y las justificaciones para su no aplicación, y los controles no aplicables en el ambiente de la organización con sus justificaciones.

Los documentos que se enumeran a continuación son los requisitos generales obligatorios y la base documental requerida para la auditoría de un SGSI:

1. Declaración de la política de seguridad y los objetivos del SGSI;
2. Alcance;
3. Procedimientos y controles;
4. Descripción de la metodología de análisis / evaluación de riesgos;
5. Informe de análisis / evaluación de riesgos;
6. Plan de tratamiento de riesgos;
7. Procedimientos necesarios para garantizar la eficacia, la operación y los controles;
8. Descripción de la medición de la eficacia de los controles;
9. Registros requeridos.

3.6 Control de documentos

» Aprobar la documentación.
» Revisar, actualizar y rechazar cuando sea necesario.
» Garantizar que los cambios y el estado de actualización estén identificados.

- Garantizar que los documentos pertinentes están disponibles en los puntos de uso en la versión más reciente.
- Garantizar que los documentos permanecen legibles y fácilmente identificables.
- Garantizar que los documentos de origen externo sean identificados.
- Garantizar que la distribución sea controlada.
- Aplicar la debida identificación en caso de que se retengan por cualquier razón.

3.7 Control de registros

Los registros deben establecerse y mantenerse para demostrar:

- La evidencia de la conformidad con los requisitos y la efectividad de la operación del SGSI.
- Conformidad con las obligaciones contractuales.

Los registros deben ser solicitados durante las entrevistas de auditoría para comprobar la ejecución de los controles.

Lea los artículos 4.3.1, 4.3.2 y 4.3.3 de la norma NTC ISO/IEC 27001:2005.

Ejercicio de refuerzo - requisitos generales de la documentación

Usando la norma ISO 27001, explique las razones de la importancia de la documentación dentro de un SGSI.

3.8 Responsabilidad de la dirección

El compromiso de la dirección de la organización es fundamental para la implementación y mantenimiento del SGSI. En cualquier actividad de seguridad de la información la participación de la alta dirección es muy importante para el éxito. Por lo tanto, el compromiso de la dirección de la organización es fundamental para la implementación y mantenimiento del SGSI. Es a través de este compromiso que los otros miembros de la organización comprenden la importancia y la necesidad de consolidar un SGSI.

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento y el mantenimiento del SGSI. Se deberá garantizar que todo el personal con responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas, proporcionando una formación adecuada y manteniendo un registro de competencias.

Lea el capítulo 5 de la norma NTC ISO/IEC 27001:2005.

3.9 Auditorías internas del SGSI

La organización debe realizar auditorías internas a intervalos planificados para determinar objetivos, controles, procesos y procedimientos del SGSI.

Una auditoría debe planificarse teniendo en cuenta el estado y la importancia de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. Se deben definir los criterios de auditoría, su alcance, frecuencia y métodos.

3.10 Análisis crítico del SGSI

Como se ha visto anteriormente, el análisis crítico es esencial para el proceso de mejoramiento. La dirección debe analizar críticamente el SGSI a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continua. Esta revisión debe incluir oportunidades de mejora y las necesidades de cambio del SGSI, incluyendo la política y objetivos de seguridad. Los resultados de esta revisión deben ser claramente documentados y los registros deben mantenerse.

3.11 Datos de entrada

Datos de entrada del análisis crítico:

- Los resultados de las auditorías internas.
- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos que se pueden utilizar en la organización para mejorar el SGSI.
- Estado de las acciones correctivas y preventivas.
- Vulnerabilidades o amenazas no contempladas.
- Resultado de indicadores del SGSI.
- Acompañamiento de las acciones de las revisiones gestionadas.
- Recomendaciones para la mejora.
- Cualquier cambio que pueda afectar el SGSI.

Estos son datos de las evaluaciones realizadas en el período y la información obtenida a partir de nuevos análisis de riesgos, de los involucrados y de observaciones.

3.12 Datos de salida

Los datos de salida de un proceso de análisis crítico son exactamente los que tienen por objetivo la búsqueda de la excelencia en el SGSI. Debe incluir todas las acciones y decisiones que se relacionan con:

- Mejora de la eficacia del SGSI.
- Actualización de análisis / evaluación y plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afectan a la seguridad de la información.

» La necesidad de recursos;
» Mejoras en el control de la eficacia del SGSI.

De esta manera se cierra un ciclo de vida del SGSI. Pero no debemos olvidar que el SGSI es un sistema de procesos continuos y formalizados, con el objetivo de proporcionar un procedimiento formal para la seguridad de la información de la organización con el fin de cumplir con sus objetivos de negocio.

3.13 Mejora del SGSI

La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de seguridad, resultados de las auditorías, el análisis de los eventos monitoreados, acciones correctivas y preventivas y la revisión de la dirección.

» **Acciones correctivas:** la organización debe tomar acciones correctivas para eliminar las causas de las no conformidades con los requisitos del SGSI para evitar su repetición.
» **Acciones preventivas:** la organización debe determinar acciones para eliminar las causas de no conformidades potenciales con los requisitos del SGSI, para prevenir su ocurrencia.

Ejercicio de refuerzo - las mejoras del SGSI

» De dos ejemplos de cada tipo de acción para la mejora del SGSI.

3.14 Controles detallados

La gestión de la seguridad de la información fomenta la adopción de políticas, procedimientos, directrices y otros elementos pertinentes, cuyo alcance debe comprender la gestión del riesgo sobre la base de costo/beneficio para la organización, entre ellos se encuentran:

» Política de seguridad de la información.
» Seguridad organizacional.
» Gestión de activos.

- Seguridad de los recursos humanos
- Seguridad física y del ambiente.
- Gestión de las operaciones y las comunicaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de SI.
- Gestión de incidentes de seguridad.
- Gestión de la continuidad del negocio.

Todos los elemento son tratados en detalle en la norma ISO / IEC 27002:2007 y se explican en capítulos específicos a continuación.

Lea las secciones 7 y 8 de la norma NTC-ISO/IEC 27001:2005.

Capítulo

04

Política de seguridad de la información

Objetivos

Identificar los requisitos, construir y utilizar una política de seguridad de la información

Conceptos

Política de seguridad, normas, procedimientos y buenas prácticas.

4.1 Definición

Inicialmente, serán vistos los siguientes temas relacionados con la política de seguridad: definición, alcance y algunas cuestiones relevantes a tener en cuenta, con miras a su desarrollo y su implementación en las organizaciones.

Ejercicio de nivelación - política de seguridad de la información

- » ¿Qué entiende usted por política?
- » En su opinión, ¿cómo debería ser una política de seguridad?

Antes de comenzar este capítulo, haga una lectura completa de la sección 5: política de seguridad de la información, de la norma ISO / IEC 27002:2005. NTC ISO/IEC 27002:2007.

La política de seguridad de la información es un conjunto de lineamientos basados en unas normas y procedimientos que determinan las reglas y procedimientos a seguir para garantizar la seguridad de la información, de acuerdo con el tipo de negocio y los requisitos legales, contractuales, regulatorios y normativos aplicables a todo el alcance de la organización. Ella establecerá las directrices, límites, responsabilidades y objetivos de los controles que se deben implementar e implantar para garantizar los requisitos de protección de seguridad de la información en la organización.

Por lo tanto, la política de seguridad debe estar claramente definida, publicada, actualizada y apoyada por los dirigentes de la organización.

La importancia de la política de seguridad para el SGSI es alta, dado que representa un documento formal, incluso con valor jurídico.

4.2 Diagrama

La política de seguridad de una organización está compuesta por directrices generales que sirven como base para las normas, los procedimientos y las instrucciones relacionadas a la seguridad de la información.

Debe estar alineada con la norma ISO 27001, con la legislación vigente y las normas generales por las que se rige la organización.

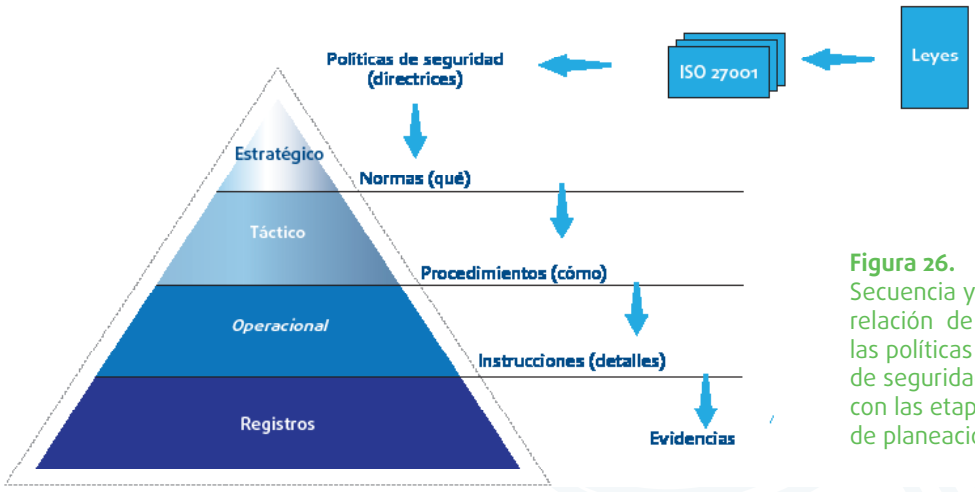


Figura 26. Secuencia y relación de las políticas de seguridad con las etapas de planeación

Tabla 1. Secuencia y relación de las políticas de seguridad con las etapas de planeación

Políticas	Directrices que se deben seguir. Responde al "por qué" realizar la seguridad de la información, definiendo directrices genéricas de lo que debe hacer la organización para lograr la seguridad de la información.
Normas	Reglas básicas de cómo debe ser implementado el control o conjunto de controles, que se definieron en las políticas. Responden "qué" hacer para alcanzar las directrices definidas en la política de seguridad.
Procedimientos	Actividades detalladas sobre cómo deben ser implementados los controles o conjunto de controles. Responde "cómo" hacer cada elemento definido en las normas específicas y sus políticas.
Instrucciones	Descripción de una operación o conjunto de operaciones para la ejecución de la implementación de los controles de seguridad de la información.
Evidencias	Mecanismos adoptados para permitir la recolección y verificación de la aplicación de los controles de seguridad de la información, su eficacia y eficiencia. Permite la trazabilidad y su uso en auditorías.

Ejercicio de refuerzo - diagrama

¿Cuáles son los procedimientos formales existentes en el departamento de las TI de su organización?

4.3 Arquitectura de políticas de seguridad

No existe una arquitectura estándar para la definición de políticas de seguridad. Ellas deben seguir y cumplir los requisitos de negocio de la organización y su cultura organizacional. Para una buena estructuración de las políticas de seguridad se puede tener como base las dimensiones de la seguridad de la información presentada en el libro "Practicando la Seguridad de la Información":

Fuente: Fontes (2012)

Figura 27. Estructura basada en la Norma Internacional ISO/IEC 27002:2007

Estas pueden ser vistas como las políticas de seguridad necesarias, pero que deben ser adecuadas a las necesidades de cada organización. Es fundamental que cada organización establezca la arquitectura que necesita tener para cumplir con los requisitos de seguridad y de negocios.

4.4 Alcance

En una organización, la política de seguridad debe:

- Establecer los principios a seguir con el fin de proteger, controlar y monitorear sus recursos y su información;
- En particular, la política de seguridad de la información puede ser integrada a otras políticas y planes existentes en la organización, como las políticas de contingencia y el plan estratégico de negocios.
- Al definir el alcance de la política, detallar los límites de su aplicación, citando los ambientes físicos, lógicos y organizacionales que son aplicables y tipos de usuarios, entre otros.

Ejercicio de refuerzo - alcance

» ¿Qué nivel de detalle es necesario para definir el alcance de la política de seguridad de su organización?

4.5 Preguntas importantes

Con el objetivo de definir una política de seguridad de la información para una organización, se debe tener en cuenta las respuestas a las siguientes preguntas:

» ¿Qué desea proteger? Activos de la organización que requieren protección.
» ¿Contra qué o quién? ¿Cuáles son las amenazas que pueden afectar a la organización y cómo y por quién estas amenazas pueden ser explotados?
» ¿Cuáles son las amenazas más probables? Identificar las amenazas que tienen más posibilidades de ocurrir.
» ¿Cuál es la relevancia de cada recurso a ser protegido? Importancia del recurso dentro del proceso de negocio.
» ¿Cuál es el grado de protección requerido? Requisitos de protección que el negocio requiere. ¿Qué nivel de protección es necesario?
» ¿Cuánto tiempo, recursos financieros y humanos están a disposición? ¿Cuáles recursos están disponibles para fines de seguridad? ¿Qué se puede hacer con los recursos existentes?
» ¿Cuáles son las expectativas de los usuarios y clientes? ¿Qué espera usted de la seguridad de la información para el negocio de la organización, servicios y productos?

Así, se pueden aplicar mecanismos de seguridad adecuados a los requisitos de seguridad indicados por la política. Además, con las respuestas adecuadas, se puede analizar los riesgos y los requisitos legales y de normas, de acuerdo con la política de seguridad.

4.6 Etapas

La política de seguridad debe implantarse de acuerdo con un proceso formal, pero flexible, para permitir cambios de acuerdo a las necesidades. Una propuesta típica para la implementación de una política de seguridad de la información comprende:

- Identificar las leyes aplicables a la organización;
- Identificar los recursos críticos;
- Clasificar la información de la organización, no sólo observando el área de informática, sino todos los sectores y su información;
- Analizar las necesidades de seguridad, con el objetivo de identificar las posibles amenazas, los riesgos y los impactos en la organización;
- Preparar la propuesta de la política de seguridad;
- Discutir abiertamente con todos los involucrados el contenido de la propuesta presentada;
- Aprobar la política de seguridad;
- Implementar la política de seguridad;
- Hacer mantenimiento, regularmente, de la política de seguridad, buscando identificar las mejoras necesarias y hacer las revisiones necesarias.

A continuación se detallan cada uno de los pasos mencionados.

4.6.1 Identificar la legislación

Cada organización está sujeta a diversas leyes, reglamentos, normas de la agencia reguladora en su área de negocio, que deben seguirse y cumplirse bajo el riesgo de sanciones en caso de incumplimiento. Por lo tanto, es importantísimo el levantamiento de toda la legislación con el fin de evitar que las políticas de seguridad atenten contra alguna de ellas.

Ejercicio de refuerzo - identificar la legislación.

¿Cuál es la importancia de la identificación de la legislación para el desarrollo de la política de seguridad?

4.6.2 Identificación de los recursos críticos

La primera fase del proceso de implementación de una de política de seguridad incluye la identificación de los recursos críticos de la organización, es decir, los recursos sujetos a riesgos de seguridad.

Por ejemplo, teniendo en cuenta los escenarios de tecnología de la información, se presentan los siguientes recursos como críticos:

- Hardware, tales como servidores, equipos de interconexión (*routers, switches*, etc), las líneas de comunicación, etc.;
- Software, tales como sistemas operativos, aplicaciones, herramientas de ayuda a actividades de negocio, utilidades, etc.;
- Datos (procesamiento o transmisión), copias de seguridad, *logs*, bases de datos, etc.;
- Personas, en términos de los usuarios (internos y externos, según sea el caso), empleados y dirigentes;
- Documentación relativa a software, sistemas de información, entre otros;
- Suministros, tales como papel, cintas, CDs / DVDs, etc.

Considerando un escenario diferente, otro tipo de recursos se pueden plantear.

Ejercicio de refuerzo - identificación de los recursos críticos

¿Nombre dos recursos fundamentales de su organización que se deben tener en cuenta en el desarrollo de la política de seguridad?

4.6.3 Análisis de requisitos de seguridad

Al analizar las necesidades de seguridad, se debe considerar el análisis de riesgos, en particular, las amenazas e impactos con el fin de determinar los elementos críticos de la organización, sus costos asociados y el nivel de seguridad adecuado.

Un análisis de riesgos completo y preciso es el punto clave para una apropiada política de seguridad de una organización, y por lo tanto para la gestión de la seguridad de la información. La gestión del riesgo se

detallará en los capítulos 6 y 7, que incluyen más información sobre el análisis de riesgos.

Otro punto a destacar son las recomendaciones de buenas prácticas en el ámbito de la seguridad de la información. El seguimiento de estas buenas prácticas ayudará a que la organización sea vista como preocupada por la seguridad de su información.

4.6.4 Preparación de la propuesta y la discusión abierta

La propuesta de una política de seguridad de una organización debe estar elaborada con base en el estudio de los recursos críticos y en el análisis de las necesidades de seguridad realizadas previamente para que, así, los objetivos de seguridad sean identificados de manera adecuada, de acuerdo con el negocio y los riesgos involucrados en la organización.

La política de seguridad debe, normalmente, ser desarrollada y presentada por el comité para la seguridad de la información. Este comité está integrado por representantes de diversas áreas, principalmente el área jurídica, de las TI y de recursos humanos, y debe tener un período establecido.

Una vez elaborada, la propuesta debe ser discutida abiertamente con todo el personal directamente involucrado con el asunto, en particular, con los dirigentes de la organización, teniendo en cuenta su apoyo es crucial para la implementación de la política de seguridad.

Ejercicio de refuerzo – preparación de la propuesta

» ¿Quién va a desarrollar la política de seguridad de su organización?

4.7 Documentación

La política de seguridad de una organización debe ser documentada, y el documento generado debe ser aprobado por sus dirigentes para que pueda ser publicado y difundido a todos los involucrados. Vale la pena mencionar la necesidad de alinear la política de seguridad con los objetivos y estrategias de negocio de la organización.

La política de seguridad debe contener, por recomendación de la norma ISO/IEC 27002:2007, los siguientes elementos:

- La definición de seguridad de la información, sus objetivos, el alcance y relevancia para la organización;
- Declaración del compromiso de los líderes de la política de seguridad de la organización;
- Indicación de los objetivos de control y de los controles, incluyendo el análisis / evaluación y la gestión del riesgo;
- Breve explicación acerca de las políticas, principios, normas y requisitos para garantizar la conformidad con la legislación, reglamentos, contratos y normas de seguridad;
- Definición de las responsabilidades con la gestión de seguridad de la información;
- Las referencias a los documentos que sustentan la política de seguridad.

Es de destacar que la política de seguridad puede estar compuesta por una serie de políticas específicas, como la política de contraseñas, *backup,* etc.

4.8 Aprobación e implementación

La fase de aprobación de la política de seguridad corresponde al resultado positivo obtenido tras el análisis de la propuesta elaborada y presentada a la organización. En particular, ésta exige el apoyo de los líderes de la organización como una forma de asegurar los primeros pasos hacia la implementación de la política de seguridad y las condiciones adecuadas para su mantenimiento.

En la implementación deben ser considerados todos los aspectos relacionados con la implementación de mecanismos de seguridad (soluciones técnicas, administrativas, etc.) apropiados para garantizar que

las necesidades de seguridad levantadas previamente son atendidas adecuadamente.

Ejercicio de refuerzo – aprobación e implementación

» ¿Quién va a aprobar la política de seguridad de su organización?

4.9 Comunicación de la política y entrenamiento

La divulgación de la política de seguridad y su comunicación a toda la organización es otro aspecto importante de su implementación en la organización. Se recomienda, a propósito, que la divulgación haga parte de la formación de los empleados nuevos y de la actualización de los antiguos, además de que se realicen periódicamente. Esta política de divulgación debe ser formal y efectiva, indicando todos los detalles de su implementación, cómo debe ser cumplida y las sanciones, en caso de incumplimiento. Recuerde que la mejor medida de prevención es la educación.

4.10 Mantenimiento

La política de seguridad de la información adoptada en una organización debe analizarse periódicamente (se recomienda anualmente), con el objetivo de mantener su idoneidad y su eficiencia. También debe ser revisado en caso de cambios significativos en cuanto a los negocios y avances tecnológicos. En el análisis se busca:

» Las mejoras a la política misma, mejoras en los controles, la asignación de recursos y la asignación de responsabilidades;
» Responder a los cambios del negocio, los recursos disponibles, condiciones técnicas y tecnológicas;
» Presentar una respuesta a los cambios que afectan directamente el modo de gerencia de la seguridad de la información;
» Responder a los cambios en los aspectos contractuales, reglamentarios y legales;
» Atender las recomendaciones de las autoridades u organismos competentes.

Se recomienda que este análisis sea realizado por un empleado o equipo responsable de la gestión de la política de seguridad. A continuación, se debe generar el nuevo documento de la política de seguridad, y este, a su vez, debe ser reconocido y apoyado por los líderes de la organización.

Ejercicio de refuerzo – mantenimiento

» ¿Cómo definir el tiempo para el mantenimiento de una política de seguridad?

4.11 Buenas prácticas

La política de seguridad tiene un papel clave en las organizaciones y, por eso, se recomienda que se considere como un conjunto de reglas que se deben seguir fielmente y se deben gestionar de manera adecuada. Por lo tanto, es evidente la relación entre la gestión de la seguridad de la información y la política de seguridad de una organización.

Para obtener mejores resultados se recomiendan las siguientes buenas prácticas, al considerar la política de seguridad de una organización:

» La alta dirección de la organización debe apoyar y creer que las políticas de seguridad de la información van a proteger su información. Por lo tanto, el patrocinio de la alta dirección es importante para que se cumplan los objetivos de la política de seguridad. Este apoyo debe comenzar con el desarrollo de la política, pasar por su firma y divulgación, llegando al mantenimiento de la eficiencia y su actualización.
» No siempre es posible detectar una violación de la política de seguridad, sin embargo, en situaciones donde hay una posibilidad, es importante identificar la causa en primera instancia como por ejemplo un error, negligencia, desconocimiento de la política, etc. Por otra parte, se recomienda que en la política de seguridad que establezcan los procedimientos a seguir si se produce una violación, según su gravedad, determinando también las acciones correctivas necesarias y sanciones a los responsables directos del problema. Tenga en cuenta que, como ya se mencionó en el capítulo 2, el castigo puede variar dependiendo de la ofensa y puede ser tratado legalmente; sin

embargo, la organización deberá divulgar la política de seguridad, la legislación vigente y las responsabilidades específicas de todos sus empleados .

» Es saludable establecer una estructura organizativa responsable de la seguridad de la información en la organización, con el fin de determinar las personas responsables de la aprobación, revisión y gestión de la implementación de la política de seguridad en la organización. Tales actividades pueden ser realizadas por un empleado o equipo.

» Se debe trabajar la seguridad del personal para minimizar o incluso evitar los problemas de seguridad de la información con causa proveniente de errores humanos.

Todos los miembros de la organización deben tener conocimiento sobre los riesgos para la seguridad y sus responsabilidades con el aspecto de seguridad. Para eso, se recomienda siempre la difusión de buenas prácticas, las normas, las leyes y normas vigentes.

4.12 Otras buenas prácticas

El control y la clasificación de los recursos informáticos de la organización son relevantes. La clasificación se lleva a cabo de acuerdo con las condiciones críticas del recurso para el negocio. En particular, se debe asociar cada recurso a un responsable directo en la organización.

La implementación del control de acceso lógico y físico para establecer los límites de acceso son recomendados, utilizando dispositivos de control de entrada y salida. En cuanto a los recursos computacionales y otros activos de la organización, es importante administrarlos de acuerdo a las exigencias actuales de seguridad de la información.

La auditoría de seguridad de la información debe ser una actividad periódica de la organización con el fin de verificar si la política de seguridad es eficiente y si hay necesidad de actualizaciones.

4.13 Buenas prácticas para escribir el texto de la política

- **Definir el objetivo del documento:** describa cuál es el objetivo del documento y lo que la organización quiere comunicar con el documento de la política.
- **Use textos cortos y objetivos:** escritos en el lenguaje del público de la organización. Sea claro en el mensaje que desea transmitir, para que el texto sea entendido por todos. Sea explícito y no deje dudas o incertidumbres.
- **Definir los roles y responsabilidades con respecto a la política de seguridad.**
- **Evitar el uso de términos técnicos o lengua extranjera:** nadie está obligado a conocer la terminología técnica que no se usa su área de especialización.
- **Evitar el uso de "no":** si es necesario, utilice "está prohibido", "negar", "está vetado", entre otros.
- **Evitar el uso de "excepto" o "en principio":** estos términos crean oportunidad para disculpas por incumplimiento.
- **Crear en la política un elemento para las definiciones y los conceptos:** definir en el principio del documento todos los conceptos, definiciones, términos técnicos y acrónimos que se utilizarán en la política.
- **Penalización:** definir las posibles sanciones para aquellos usuarios que no cumplan con la política. Solicitar la colaboración de la oficina jurídica y recursos humanos.
- **Crear reglas y recomendaciones factibles de ser implementadas y cumplidas por toda la organización y en todos los niveles jerárquicos.**
- **Tenga cuidado con la estructura gramatical:** las políticas deben ser ejemplo de un texto escrito correctamente. Evite los modismos y los términos de doble sentido.
- **Solicitar que la oficina jurídica evalué el documento y certifique su aceptación.**

Directrices para el desarrollo de la política de seguridad de la información y comunicaciones en los órganos y entidades de la Administración Pública en Colombia

En el artículo 227 de la Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo 2010-2014, señala que para el ejercicio de sus competencias las entidades públicas y los particulares que cumplen con funciones públicas deberán poner a disposición de la Administración Pública, bases de datos de acceso permanente y gratuito con la infor-

mación que producen y administran. De igual forma, el parágrafo 3 del mismo artículo señala que el Gobierno Nacional debe garantizar, mediante la implementación de sistemas de gestión para la seguridad de la información, que el acceso a las bases de datos y la utilización de la información sean seguros y confiables para no permitir su uso indebido.

En el año 2003 la Dirección Nacional de informática y Comunicaciones, DNIC, de la Universidad Nacional de Colombia emitió internamente una "Guía para la elaboración de Políticas de Seguridad" como una metodología potencialmente útil para el desarrollo, implementación, mantenimiento y eliminación de un conjunto completo de políticas tanto de seguridad como en otras áreas.

Se recomienda leer el documento completo, al cual se puede acceder en:
http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf

Capítulo

05

La gestión del riesgo

Objetivos

Comprender, describir y evaluar el proceso de gestión del riesgo.

Conceptos

Definición de la gestión del riesgo, el análisis/evaluación de riesgos y la aceptación, el procesamiento y la comunicación de los riesgos.

5.1 Definiciones

Ejercicio de nivelación – gestión del riesgo

» ¿Qué es riesgo para usted?
» ¿Qué entiende usted por gestión del riesgo?

Riesgo de seguridad es una combinación de amenazas, vulnerabilidades e impactos. Las amenazas son eventos que aprovechan las vulnerabilidades (debilidades) y pueden causar daños. El impacto es el resultado de una vulnerabilidad al ser explotada por una amenaza.

En cuanto a la gestión del riesgo, algunas definiciones se consideran importantes y se presentan a continuación:

» La gestión del riesgo incluye todas las medidas adoptadas para controlar los riesgos en una organización, incluyendo el análisis/evaluación, el tratamiento, la aceptación y la comunicación de los riesgos.
» El análisis de riesgos identifica y estima los riesgos, teniendo en cuenta el uso sistemático de la información. Abarca el análisis de las amenazas, vulnerabilidades e impactos y se considera el punto clave de la política de seguridad de la información de una organización.
» La evaluación del riesgo compara el riesgo estimado en el análisis con los criterios predefinidos con el fin de identificar la importancia de cada riesgo para la organización.
» Aceptación de riesgos incluye la identificación del nivel aceptable de riesgos para una organización en función de sus necesidades específicas de negocio y seguridad.
» El tratamiento del riesgo corresponde a la selección y la aplicación de medidas para modificar un determinado riesgo.

La comunicación de riesgos involucra iniciativas para mostrar los riesgos a los empleados, directivos y terceros (estos últimos, cuando sea apropiado y necesario).

5.2 Cuestiones claves

Para llevar a cabo una gestión eficaz del riesgo, es necesario identificar inicialmente, las amenazas y los impactos, la probabilidad de la materialización de las amenazas y riesgos potenciales. Se recomienda clasificar los riesgos según los criterios: nivel de importancia, gravedad de las pérdidas y costos involucrados en la prevención o recuperación de desastres.

Si el costo para evitar una amenaza es mayor que su daño potencial, es aconsejable tener en cuenta otras medidas. Las decisiones deben ser tomadas teniendo en cuenta la importancia que tiene para la continuidad del negocio de la organización el activo amenazado.

Tenga en cuenta que el análisis de las amenazas y vulnerabilidades busca identificar la probabilidad de ocurrencia de cada evento adverso y las consecuencias de los daños, mientras que el análisis de impacto debería identificar los recursos críticos para la organización; es decir, los que más sufren con los daños.

Dado que es muy difícil definir con precisión la probabilidad de que una amenaza ocurra y los respectivos daños causados, se recomienda establecer una lista de amenazas potenciales, de los recursos afectados, de los requisitos de seguridad afectados y el grado de impacto (por ejemplo, muy alto, alto, moderado, bajo y muy bajo).

5.3 La gestión del riesgo

La gestión del riesgo debe considerar los siguientes tres niveles de aplicación: tecnologías, procesos y personas. La tecnología garantiza los ajustes técnicos necesarios para el tratamiento adecuado de los riesgos; los procesos de asegurar que las actividades que componen la gestión de los riesgos sean consideradas de forma sistemática, y, por último, las personas, de modo que los empleados y los gerentes identifiquen sus responsabilidades, conozcan los riesgos y puedan ayudar a su reducción y control. Instrumentos como la política de seguridad y un código de conducta se recomiendan en su contexto.

En cuanto a las medidas de seguridad, se recomienda atención a las siguientes categorías: preventivas, de carácter estructural (por ejemplo, una política formal para el control de acceso lógico); correctivas, como una emergencia (planes de contingencia, por ejemplo), e ilustrativas, con carácter educativo (entrenamientos, folletos, conferencias, etc.).

En particular, recuerde que la orientación y la información son esenciales para la reducción de riesgos. Por lo tanto tenga en cuenta la importancia del siguiente flujo de gestión del riesgo: información - conocimiento - cambio de conducta - educación - prevención de los riesgos.

Figura 28. Secuencia para el cambio de comportamiento y la prevención de riesgos

Ejercicio de refuerzo - gestión del riesgo

» ¿Cuáles son los tres niveles a tener en cuenta en la gestión del riesgo?

5.4 Análisis y evaluación de riesgos

En esta sección, se presentan los aspectos relevantes para el análisis/evaluación de los riesgos en las organizaciones. En particular, se presentarán algunas clasificaciones para análisis de impacto, definición de probabilidades y cálculos de riesgo.

Identifica, califica/cuantifica y prioriza los riesgos de seguridad de la información. Es esencial para:

» Gestión del riesgo.
» Proposición de medidas de seguridad apropiadas.

Consideraciones:

» Deben ser sistemáticas.
» Deben utilizar métodos concretos.
» Se deben realizar periódicamente.

El análisis/evaluación de riesgos consiste en identificar, cuantificar y calificar los riesgos de seguridad de la información, con base en los objetivos de la organización. Incluye también la priorización de los riesgos, teniendo en cuenta los criterios de riesgo aceptable. Es una actividad que indica la forma de garantizar una gestión adecuada de la información sobre riesgos de seguridad y un conjunto adecuado de medidas de seguridad de la organización en cuestión.

Algunos aspectos de análisis / evaluación de riesgos que deben ser contemplados son:

- Deben ser llevados a cabo de manera sistemática con el fin de identificar los riesgos (análisis) y calificar el riesgo (evaluación). El análisis de riesgo mide las amenazas, vulnerabilidades, impactos y actividades en un ambiente determinado con el fin de orientar la adopción de las medidas adecuadas al negocio y a los requisitos de seguridad de la organización.
- Debe utilizar métodos específicos para permitir la comparación entre los resultados obtenidos y su reproducción.
- Debe realizarse periódicamente o cuando los requisitos de seguridad, activos, vulnerabilidades y / o los objetivos de negocio sufren algún cambio.

5.5 Analizando los riesgos

El análisis de riesgo debe considerar los daños probables al negocio resultantes de fallas de seguridad; la probabilidad de que las fallas ocurran frente a las vulnerabilidades y amenazas existentes; y las medidas de seguridad implementadas (si es aplicable) para que al final, se recopilen los datos necesarios para la adecuada gestión del riesgo.

Por lo tanto, algunas preguntas deben ser contestadas:

- ¿Qué hay que proteger?
- ¿Cuáles son las vulnerabilidades y amenazas?
- ¿Cómo analizar?

La respuesta a estas preguntas es esencial para la ejecución y generación de resultados en el análisis de riesgos.

5.6 ¿Lo que hay que proteger?

En esta etapa, se deben considerar todos los activos involucrados en el alcance del SGSI de la organización, especialmente los directamente relacionados con los objetivos del negocio. Por lo tanto, se trata de una fase que no puede ser subjetiva, es decir, se recomienda hacer un inventario cuidadoso de los activos, teniendo en cuenta parámetros y categorías de selección, por ejemplo.

En particular, usted debe examinar primero las amenazas y vulnerabilidades de los activos a ser protegidos, de modo que sean considerados todos los eventos adversos que tal vez pueden explotar las debilidades de seguridad de la organización, causando daños.

Hardware, software, datos, personas, documentos, sistemas de información, contratos, entre otros, son ejemplos de activos considerados cruciales para el negocio de la organización.

Ejercicio de refuerzo -qué proteger

» Cite ejemplos de activos críticos en su organización.

5.7 Vulnerabilidades y amenazas

Después de identificar los activos que deben ser protegidos en la organización, se deben considerar las probabilidades de cada activo de ser vulnerable a las amenazas. Para ello, hay que prestar atención a la información que pueda quedar comprometida, creando listas de prioridades, por ejemplo; y los servicios de seguridad que puedan verse comprometidos, tal como la confidencialidad, integridad y disponibilidad.

Ejemplos de amenazas típicas:

» Desastres naturales.
» Falta de suministro de energía eléctrica.
» Robo/estafa
» Amenazas programadas.
» Fallas de hardware.
» Fallas de software.
» Errores humanos.

A continuación se presentan algunas de las amenazas típicas en entornos de las TI:

- Los desastres naturales que afectan a la instalación física de la organización. Durante el desastre, los controles de acceso físico pueden verse comprometidos y algunos recursos con información sensible se pueden violar con facilidad.
- Las fallas en el suministro eléctrico, que afectan a la parte de hardware de la organización. Con el hardware dañado, los servicios no estén disponibles.
- Amenazas programadas tales como virus y bombas lógicas que afectan software. Por lo tanto, los códigos no autorizados pueden revelar la información confidencial al mundo exterior, tal como contraseñas.
- Las fallas de hardware. De este modo, la máquina comprometida puede ser enviada a mantenimiento sin el previo cuidado de borrar la información confidencial contenida en los mismos.
- Las fallas de software, corrompiendo lo datos.
- Los errores humanos que afectan a cualquier sistema de la organización, permitiendo así la revelación de información confidencial; por ejemplo, imprimir información confidencial en una impresora pública.

El análisis de riesgos debe medir las amenazas, las vulnerabilidades y los impactos de modo que el resultado pueda servir como guía para la adopción de medidas de seguridad adecuadas a los requisitos de negocio de la organización, teniendo en cuenta, por lo tanto, costos asociados, nivel de protección requerido por los activos y facilidad de uso.

En particular, se puede considerar el análisis de riesgos en términos cualitativos, con el fin de cumplir con los requerimientos del negocio, o en términos cuantitativos, con el fin de asegurar que los costos de las medidas preventivas, correctivas e ilustrativas no superen el valor del activo en cuestión, en lo que se refiere al patrimonio de la organización y también a la continuidad del negocio.

Tabla 2. Datos de ejemplo para una organización en particular

Tipo de datos	Clasificación	Importancia
Resultado clínico	Búsqueda	Alto
Estudio de mercado	Búsqueda	Bajo
Patentes dependientes	Propietario	Alto
Memorandos	Administrativo	Bajo
Los sueldos de los empleados	Financiero	Medio
Características de producto nuevo	Propietario	Medio

En el ejemplo, se consideró que el activo "datos" y además los objetivos de negocio de una organización determinada para establecer una clasificación de los datos (administrativos, financieros, cliente, investigación, propietario) y la debida importancia dada a cada categoría.

5.8 Análisis de los impactos

El impacto es el resultado cuando se produce una amenaza. Así, por ejemplo, teniendo en cuenta los controles de acceso inadecuados, podemos mencionar los impactos tales como la modificación no autorizada de datos y aplicaciones y la revelación no autorizada de información, lo cual, a su vez, causa problemas directos para la organización. Por lo tanto, es importante analizar los impactos, con miras a la gestión apropiada de riesgos dentro de la organización.

Para el análisis de los impactos, se puede considerar una propuesta de clasificación específica de apoyo. Por lo general, los impactos de las amenazas a la organización se analizan desde dos aspectos: a corto y largo plazo, teniendo en cuenta el periodo de tiempo durante el cual un impacto permanece afectando a los negocios.

Se puede considerar la siguiente propuesta para categorizar los impactos:

- 0. impacto irrelevante;
- 1. Efecto poco significativo que no afecta la mayoría de los procesos de negocio de la institución;
- 2. Los sistemas no están disponibles por un determinado período de tiempo, puede causar la pérdida de credibilidad e imagen

de la organización además de pequeñas pérdidas financieras;
» 3. Pérdidas financieras a gran escala y la pérdida de clientes;
» 4. Efectos desastrosos, pero que no comprometen la supervivencia de la organización;
» 5. Efectos desastrosos que comprometen la supervivencia de la organización.

Ejercicio de refuerzo - análisis de impacto

» Explique qué es un análisis de impacto

5.9 Matriz de relaciones

La matriz de relaciones es una forma simplificada de visualizar las amenazas, impactos y las probabilidades de acuerdo con el ejemplo propuesto, es decir, en relación con cada amenaza potencial en la organización, su impacto y probabilidad de ocurrencia. Por ejemplo, las categorías de 0 a 5 para cada elemento se pueden usar, como se discutió anteriormente.

Tabla 3. Amenazas versus Impactos versus Probabilidades

Amenazas	Impacto	Probabilidad
Errores humanos		
Instalación de hardware y software no autorizado		
Códigos maliciosos		
Errores en los sistemas operativos		
Invasión		
Desastres naturales		
Desastres causados por personas		
Fallas del equipo		
Sabotaje		
Chuzadas telefónicas		
Monitoreo del tráfico de la red		

Contuniación tabla 3. Amenazas versus Impactos versus Probabilidades

Amenazas	Impacto	Probabilidad
Modificación de la información		
Acceso a los archivos de contraseñas		
Uso de contraseñas débiles		
Monitoreo del tráfico de la red		
Usuarios internos que practican actos ilegales		

Ejercicio de refuerzo - la matriz de relación

» Rellene el cuadro anterior de Amenazas X Impacto X Probabilidad con valores de 0 a 5 de acuerdo con el entorno de las TI de su organización

5.10 Cálculo del riesgo

Los riesgos se calculan a partir de la relación entre el impacto y probabilidad de ocurrencia, es decir, riesgo = impacto * probabilidad

En particular, teniendo en cuenta las calificaciones de impacto y probabilidad presentado anteriormente, al realizar la multiplicación, obtenemos un rango de valores para el riesgo del 0 (sin riesgo) a 25 (muy alto riesgo). Entonces se puede considerar esta propuesta general, por ejemplo, para el cálculo de los riesgos generales de la organización y proponer las medidas de seguridad adecuadas a su debido tratamiento, teniendo en cuenta, por lo tanto, un nivel aceptable de riesgo, dado que no todos los riesgos debido a los costos, tienen la garantía de ser reducidos por medio de medidas de seguridad.

5.11 La evaluación de riesgos

Al evaluar los riesgos se busca una base que sirve para fines de comparación, por ejemplo, el análisis y la evaluación de riesgos realizada en temporadas anteriores. El conocimiento previo de los impactos y las probabilidades de riesgo siempre es relevante para una evaluación adecuada y completa.

Por otro lado, hay básicamente dos formas de realizar la evaluación del riesgo:

- **Cualitativo:** evaluación de riesgos a través de la estimación cualitativa es la que utiliza calificadores y atributos descriptivos para evaluar. No se asignan valores financieros. Se considera muy subjetiva. Ejemplo: Alto, Medio, Bajo, Muy Bajo.
- **Cuantitativo:** evaluación de riesgos a través de una estimación cuantitativa es aquella que utiliza valores numéricos financieros para cada uno de los componentes recolectados durante la identificación de los riesgos. Ejemplo: 50% de probabilidad; el impacto: $ 100.000.000.

En los siguientes ejemplos se hacen dos análisis de riesgo realizados en el mismo entorno, pero con diferentes formas de calcular el riesgo. Tenga en cuenta los criterios que se utilizan en cada uno.

5.11.1 Ejemplo 1: análisis de riesgos

En una Institución de Educación Superior, IES, se decidió que el área de las TI llevara a cabo una evaluación de riesgos de la red administrativa en tres departamentos: ingeniería, finanzas y administración. Para esto se utilizó como metodología el concepto de riesgos como consecuencia de la probabilidad multiplicada por el impacto, con los parámetros cualitativos alto, medio y bajo, con los pesos asignados a cada uno para el cálculo del riesgo. Después de realizar la etapa de análisis de los riesgos, usted realizó la evaluación de riesgos, llegando al resultado a continuación:

Tabla 4. Los resultados de la evaluación de riesgos.

Área	Probabilidad de que ocurra		Impacto en caso de producirse		Riesgo = P x I	
	Evaluación	Peso	Evaluación	Peso	Evaluación	Peso
Departamento de ingeniería	Media	2	Medio	2	4	Medio
Departamento administrativo	Media	2	Bajo	1	2	Bajo
Departamento financiero	Media	2	Alto	3	6	Alto

Tabla 5. Criterio utilizado de probabilidad

Criterio de probabilidad		Peso
Alta	Ha ocurrido con frecuencia mensual	3
Media	Ocurrió al menos una vez en los últimos seis meses	2
Bajo	No hay registro/historia de ocurrencia	1

Tabla 6. Criterio utilizado de impacto

Criterio de impacto		Peso
Alto	Si ocurre causará grandes pérdidas financieras	3
Medio	En este caso las pérdidas causan impacto financiero hasta $10.000000	2
Bajo	En este caso las pérdidas no causarían impacto financiero	1

Tabla 7. Criterio utilizado de riesgo

Riesgo	
Alto	>4
Medio	> 2 y ≤4
Bajo	≤2

5.11.2 Ejemplo 2: análisis de riesgos

En una IES se determinó que el área de las TI realizará una evaluación de riesgo de la red administrativa en tres departamentos: ingeniería, finanzas y administración. Para esto fue utilizada una metodología desarrollada por una firma consultora que calcula los riesgos de la institución a través de una fórmula que utiliza parámetros como la criticidad, la disponibilidad, la confidencialidad entre otros. Después de realizar la etapa de análisis de los riesgos, usted realizó la evaluación de riesgos, llegando al siguiente resultado.

Tabla 8. Resultado de la evaluación de riesgos

Área	Criticidad de la red	Disponibilidad de la red	Confidencialidad de la red	Importancia de la red	EO	ED	RR
Departamento de ingeniería	2	3	1	6	0.1	0.3	3.8
Departamento administrativo	2	3	2	12	0.5	0.5	3.0
Departamento financiero	2	3	3	18	0.3	0.3	8.8

Tabla 9. Los valores de los criterios de criticidad, disponibilidad y confidencialidad

Riesgo	
Alto	> 4
Medio	> 2 y ≤4
Bajo	≤2

Tabla 10. Valores para evitar la ocurrencia y la degradación

Valores EO y ED	
Muy baja	0.1
Bajo	0.3
Moderado	0.5
Alto	0.7
Muy alto	0.9

Tabla 11. Convenciones utilizadas

Convenciones		
IR	Importancia de la Red	¿Cuál es la importancia de la red para los negocios?
EO	Evitar la Ocurrencia	¿Cuál es la probabilidad actual de evitar la ocurrencia?
ED	Evitar la Degradación	¿Cuál es la capacidad actual para prevenir la degradación?
RR	Riesgo Relativo	IR*[(1-ED)*(1-ED)]Cálculo del riesgo en esta metodología

Para el ejemplo mostrado, el activo analizado es la red de la organización. Como se puede ver, ciertas convenciones se han utilizado para mapear la importancia de los servicios específicos de seguridad, tales como la disponibilidad, integridad y confidencialidad en un análisis, y en el otro sólo la probabilidad y el impacto. Al final, el resultado expresado se genera a partir de la propuesta para la medición de los riesgos de esa organización.

Determina los criterios para indicar si un riesgo es aceptable. Aspectos a tener en cuenta:

- Los requisitos legales y de seguridad.
- Los objetivos organizacionales.
- Costo x beneficio.

Esta es una actividad que tiene por objeto determinar los criterios a considerar para indicar si un riesgo es aceptable o no para la organización.

Un riesgo se considera aceptable cuando, por ejemplo, después de la evaluación, se considera bajo o su tratamiento representa costos no viables para la organización.

Para determinar si un riesgo es aceptable o no, algunos aspectos deben tenerse en cuenta:

- Los requisitos legales, reglamentarios, contractuales y de seguridad;
- Objetivos de negocio;
- Relación costo-beneficio para la adquisición/implementación de las medidas de seguridad en relación con los riesgos que deben ser reducidos.

Ejercicio de refuerzo - evaluación de riesgos

- ¿Qué es y cómo se debe determinar el riesgo aceptable?

5.12 El tratamiento de los riesgos de seguridad

Después de la revisión, evaluación y definición de criterios aceptables para los riesgos en la organización, se debe indicar el procedimiento para el tratamiento de los riesgos. Entre las alternativas de tratamiento se destacan:

- Seleccionar y aplicar las medidas de seguridad adecuadas para reducir los riesgos a un nivel aceptable (según los criterios definidos en la "Aceptación del Riesgo");
- Implementar medidas de prevención frente a los riesgos, no permitiendo que las vulnerabilidades sean explotadas para la materialización del riesgo;
- Transferir los riesgos a terceros mediante contratos con las compañías de seguros, por ejemplo.

Recuerde que los riesgos de seguridad varían según la ubicación (escenario o contexto) y, por lo tanto, es importante tener en cuenta este hecho para determinar las medidas de seguridad más adecuadas.

Preste atención al implementar medidas de seguridad, dependiendo de la organización, estas pueden ser no viables. Por ejemplo, la aplicación de registros (*logs*) para todas las actividades del usuario puede ir en contra de la legislación vigente y la privacidad de las personas en su entorno de trabajo.

Es de destacar también que supervisar, evaluar y proponer mejoras regularmente en las medidas de seguridad y, por lo tanto, el tratamiento del riesgo, es bueno para aumentar la eficacia de las prácticas de gestión del riesgo en la organización.

Ejercicio refuerzo - tratamiento de los riesgos de seguridad

- ¿Cuáles son los objetivos del tratamiento del riesgo?

El tratamiento del riesgo es una actividad que se realiza después de la análisis/evaluación de riesgos de la organización, con el objetivo de ayudar a reducir los riesgos a un nivel aceptable. Por lo tanto, el uso de procedimientos y medidas de seguridad debe aplicarse en esta actividad, bien sea con medidas preventivas, correctivas o ilustrativas.

Es de destacar que cualquier medida que implica un seguimiento regular de las personas y/o sistemas debe ser implementado de acuerdo con la legislación vigente.

En cuanto al tratamiento de los riesgos de seguridad, algunas áreas se consideran esenciales para la organización para garantizar sus objetivos de negocio. Se destacan entre estas áreas, las preocupaciones como riesgos, impactos y el debido tratamiento para recursos humanos, seguridad de acceso y de comunicaciones, además de los negocios.

- Seguridad de recursos humanos.
- Seguridad de acceso.
- Seguridad de las comunicaciones.
- Seguridad y negocios.

Ejercicio de refuerzo - tratamiento de los riesgos

- ¿Cuáles son las áreas claves de su organización para asegurar sus objetivos de negocio?

En este tema serán presentados varios ejemplos de los riesgos, los impactos y los tratamientos adecuados para garantizar que las organizaciones contemplan la seguridad en términos de recursos humanos, controles de acceso, la comunicación y los negocios.

Es de destacar que existen otras preocupaciones relevantes sobre los riesgos y los impactos en los organismos de seguridad, sin embargo, fueron tratados en este capítulo los cubiertos en la norma ISO/IEC 27002:2007 y aplicables independientemente de la rama de negocio de la organización.

5.13 Tratamiento de los riesgos en la seguridad de los recursos humanos

Las personas deben ser conscientes de sus responsabilidades y los riesgos y amenazas de seguridad. También debe estar alerta a los eventos adversos que representan riesgos.

Una buena práctica se recomienda para minimizar los riesgos de seguridad en las organizaciones y educar, sensibilizar y capacitar (cuando sea necesario) los recursos humanos: empleados, contratistas, socios, etc. En particular, algunas prácticas también ayudan a lograr este objetivo:

- Asegurar que las personas conozcan, entiendan y cumplan con sus responsabilidades en la reducción de los riesgos de seguridad de la organización, especialmente en términos de robo, fraude y el uso indebido de los recursos y la información;
- Las personas deben ser conscientes de que es importante notificar a sus superiores sobre cualquier evento adverso que represente riesgos (potenciales o reales) para la seguridad de la organización;
- Las personas deben conocer los posibles riesgos y amenazas de seguridad con el fin de comprender su papel en lo que se refiere a seguridad de la información en la organización. En particular, cada uno debe hacer sus acciones de acuerdo con la actual política de seguridad, lo que reduce la ocurrencia de errores humanos y por lo tanto los riesgos.

Ejercicio de refuerzo - tratamiento de los riesgos en la seguridad de los recursos humanos

- ¿Qué medidas va a proponer para el tratamiento de los riesgos de seguridad de los recursos humanos en su organización?

5.14 El tratamiento del riesgo en la seguridad de acceso

Al considerar la seguridad de acceso, en un principio hay una preocupación relevante con factores de riesgo para el contexto, tal como las responsabilidades asignadas a los empleados y terceros, el valor de los activos accesibles y derechos sobre el cierre de las actividades, por ejemplo.

En las organizaciones, el nivel de protección que requieren los distintos controles de acceso está determinado por el análisis/evaluación de riesgos. Por lo tanto, se debe prestar atención a los resultados obtenidos con esta actividad para determinar las medidas de seguridad adecuadas con el fin de, por ejemplo:

- Definir los perímetros de seguridad para la seguridad física y el ambiente;
- Proteger adecuadamente los equipos (internos o externos a las instalaciones de la organización) contra acceso no autorizado, pérdida o daños, peligros del propio ambiente, fuga de información, entre otros;
- Evaluar si es adecuado destruir cierto dispositivo que almacena la información crítica para el negocio de la organización, o si es apropiado enviarlo para su reparación en el lugar autorizado por el fabricante del dispositivo;
- Reducir al mínimo el riesgo de corrupción de los sistemas operativos, garantizando que la actualización se lleve a cabo sólo por personas competentes y autorizadas;
- Reducir el riesgo de amenazas tales como robo, incendio, explosiones, polvo, efectos químicos, inundaciones, fallas en suministro de energía eléctrica, etc.
- La educación y la sensibilización de los usuarios es fundamental para la seguridad de la información, dado que el uso adecuado de los recursos y la información, como "herramientas" de trabajo, fortalece la cultura de seguridad de la organización en conjunto.

Hay una serie de riesgos relacionados directamente con el control inadecuado de acceso lógico a los recursos de información. He aquí algunos ejemplos: la divulgación no autorizada de la información; modificaciones no autorizadas a los datos y aplicaciones y la introducción de los códigos maliciosos en los sistemas.

Así, la ausencia o la insuficiencia de los controles de acceso lógico afectan directamente a los recursos y la información, aumentando los ries-

gos. Por otra parte, los impactos pueden ser más grandes dado que consideramos las aplicaciones y la información crítica para el negocio de la organización. Si existen obligaciones legales involucradas con el control de acceso lógico, la organización puede sufrir demandas.

Como se ve en el ejemplo anterior, es importante tener en cuenta las medidas de seguridad adecuadas para efectuar el control de acceso lógico en las organizaciones. Por lo tanto se recomiendan algunas prácticas:

- La restricción y monitoreo del acceso a los recursos críticos de la organización, tales como servidores, documentos, etc.;
- El uso de cifrado fuerte, asegurando la confidencialidad de la información;
- No guardar las contraseñas en los *logs* debido a que permite el posterior acceso de personas no autorizadas;
- Concientizar a las personas de no divulgar sus contraseñas, ya sea verbalmente o por correo electrónico, ni almacenarlas en archivos;
- Conceder acceso a las personas solamente a los recursos que son necesarios para ejecutar sus actividades.

Existen varios riesgos relacionados directamente con el control inadecuado de acceso físico en las organizaciones. Algunos ejemplos: el robo de los equipos o sus componentes internos y los actos de vandalismo como el corte de cables eléctricos. Así, la ausencia o la insuficiencia de los controles de acceso físico también pueden facilitar el trabajo a los invasores que atacan directamente a los controles de acceso lógico aplicados a los recursos de información.

Ejemplos de tratamientos para un adecuado control de acceso físico:

- Identificar a los empleados y visitantes.
- Controlar la entrada/salida de equipos.
- Supervisar el desempeño del personal de limpieza, mantenimiento y vigilancia.

Como se ve en el ejemplo anterior, es importante tener en cuenta las medidas de seguridad adecuadas para llevar a cabo el control de acceso físico en las organizaciones. Por lo tanto, se recomiendan algunas prácticas:

- Establecer formas de identificación que distingan entre empleados y visitantes;
- Controlar la entrada y salida de equipos, registrando por ejemplo, la fecha, la hora y el responsable;

» Supervisar las actividades de los equipos de limpieza, mantenimiento y vigilancia, sobre todo si son tercerizados.

Existen varios riesgos directamente relacionados con el control ambiental inadecuado o inexistente. Como ejemplos, considere los desastres naturales y fallas en el suministro de electricidad.

Los impactos incluyen daños a los equipos, la pérdida de datos o la falta de disponibilidad de los servicios, por ejemplo, generando pérdidas financieras y de imagen de la organización.

Ejercicio de refuerzo – el tratamiento del riesgo en la seguridad de acceso

» ¿Qué riesgos en la seguridad de acceso puede identificar dentro de su entorno en su organización?
» ¿Qué medidas va a proponer para el tratamiento de los riesgos en la seguridad de acceso de su organización?

5.15 El tratamiento de los riesgos en seguridad de las comunicaciones

Para garantizar la seguridad de las comunicaciones, es importante tener en cuenta el análisis/evaluación de riesgos con el fin de adecuar las medidas de seguridad a los requisitos de información necesarios para el negocio de la organización. También se recomienda la gestión de las comunicaciones.

En este contexto, se recomiendan algunas prácticas:

» Las conexiones seguras que proporcionan servicios de red, especialmente los que operan directamente con la información crítica y las aplicaciones de negocio de la organización;
» Identificar las medidas de seguridad adecuadas para la comunicación inalámbrica, tales como autenticación fuerte y selección de frecuencias;
» Establecer la revisión periódica de los derechos de acceso a la red y sus servicios, asignados a los empleados, contratistas, colaboradores etc.

Ejercicio de refuerzo - el tratamiento de los riesgos en seguridad de las comunicaciones

» ¿Qué medidas va a proponer para el tratamiento de los riesgos en la seguridad de las comunicaciones en su organización?

5.16 El tratamiento de riesgos y el negocio

La seguridad de la información debe ser adecuada para garantizar la protección de los recursos y la información de la organización, de acuerdo con sus objetivos de negocio. En este contexto, algunas consideraciones deben ser tenidas en cuenta. Por ejemplo:

» Los riesgos relacionados directamente con aplicaciones críticas de negocio, en términos principalmente de la utilización de los recursos y la información compartida;
» Gestionar adecuadamente las nuevas situaciones que influyen en el intercambio de información y recursos, tal como los nuevos contratos o sociedades, con el objetivo de tratar los posibles riesgos de acceso no autorizado;
» En cuanto al uso de la criptografía, se debe considerar el tipo y calidad de los algoritmos adecuados a las necesidades. Es aconsejable desarrollar una política que aclare el modo de funcionamiento correcto, lo que reduce el riesgo de un mal uso, por ejemplo;
» Todos los cambios deben ser controlados, y los riesgos y los impactos involucrados deben ser considerados para determinar las medidas de seguridad adecuadas;
» En particular, la gestión de la continuidad del negocio debería incluir mecanismos para identificar y reducir los riesgos, para complementar el análisis / evaluación global de riesgos, ayudando fácilmente procesos que requieren respuestas inmediatas.

Las copias de seguridad (*backups*) son una herramienta importante para apoyar la continuidad de los servicios y por lo tanto el negocio; sin embargo, los riesgos asociados con los procedimientos inadecuados de copias rutinarias de seguridad regulares causan impactos tal como desperdicio de tiempo y recursos, y, en consecuencia, pérdidas financieras. Por ello, se recomienda a las organizaciones tomar medidas tales como una política formal de copia de seguridad y la capacitación y sensibilización continúa de los empleados en cuanto a seguridad (incluyendo orientación sobre copias de seguridad personales).

Los siguientes son algunos riesgos e impactos que se presentan relacionados directamente con problemas con la contratación de servicios de terceros. Entre los riesgos, podemos destacar la incertidumbre de que el tercero (o prestador de servicios) emplee medidas de seguridad acordes con las adoptadas en la organización, teniendo en cuenta todas las normas de la organización.

Ejemplos de tratamiento para el control adecuado de la contratación de terceros:

- Definir cláusulas contractuales que responsabilicen al tercero por la seguridad.
- Definir cláusulas contractuales que permitan actualizaciones en los servicios y sistemas.

Para hacer frente a los riesgos como los presentados en el ejemplo anterior, algunas medidas se recomiendan: establecer cláusulas contractuales que definen claramente las responsabilidades del tercero relacionadas con la seguridad de la organización, e incluir cláusulas contractuales que permitan cambios en los servicios y sistemas en función de los nuevos objetivos de negocio.

Para pensar

Un contrato de prestación de servicios deberá incluir al menos los siguientes elementos: costos básicos, los derechos de las partes (al final del contrato); compensación en caso de pérdida, los derechos de propiedad de la información, los derechos de propiedad intelectual, la transferencia de la información y la documentación técnica; posibilidad de cambio, las normas de seguridad de la organización y las normas de calidad.

Ejemplos de cláusula contractual de seguridad de la información:

"Es obligación del **contratista** siempre que utilice el sistema con una conexión a los sistemas del **contratante:** cuando así lo solicite por escrito al **contratante,** realizar los cambios necesarios para remediar los problemas potenciales de seguridad o de vulnerabilidad en los sistemas que han sido notificados por el **contratante.**"

El control de la organización consta de todos los aspectos relacionados con la protección de la organización, de acuerdo con sus objetivos teniendo como base los riesgos, tales como: violación no autorizada de acceso a los recursos de información, el robo de los equipos y la planificación inadecuada del crecimiento computacional.

Ejemplos de tratamiento para el control adecuado de la organización:

- Definir las responsabilidades de cada cargo en la jerarquía de la organización.
- Cumplir con la legislación vigente.

Para el ejemplo anterior, algunas recomendaciones sobre las medidas de seguridad son directamente aplicables:

- Definir las responsabilidades de los cargos de acuerdo con la jerarquía de la organización, de manera que las actividades se lleven a cabo correctamente.
- Cumplir con la legislación vigente y los requisitos contractuales y reglamentarios relativos a la seguridad en la organización.

Un control adecuado de cambios en las organizaciones debe proporcionar soluciones a los riesgos tales como:

- El uso de hardware y software no autorizado;
- Dificultad de mantenimiento debido a la falta de documentación y procedimientos;
- Los cambios inesperados o accidentales.

Se proponen algunas medidas de seguridad para el control adecuado de los siguientes cambios:

- Documentar todos los cambios y actualizaciones realizadas y ponerlas en práctica sólo con la debida autorización;
- Evaluar el impacto de los cambios antes de implementarlos;
- Definir el procedimiento en situaciones de emergencia;
- Planificar cambios para minimizar el impacto en el día a día de la organización.

5.17 La comunicación de riesgos

Esta actividad abarca todas las acciones para la divulgación de los riesgos, con el fin de informar y orientar a los participantes, buscando con ello la reducción (y, a menudo la eliminación) del riesgo en la organización.

Capítulo

06

Gestión de operaciones y comunicaciones

Objetivos

Describir responsabilidades, seleccionar y aplicar controles y procedimientos de gestión de operaciones y comunicaciones.

Conceptos

Definición, procedimientos y responsabilidades de la gestión de operaciones y la gestión de la seguridad de la red.

Ejercicio de nivelación -gestión de las operaciones y las comunicaciones

» ¿Qué entiende usted por gestión de operaciones y comunicaciones?
» ¿Cómo realiza su organización la gestión de las operaciones y las comunicaciones?

6.1 Objetivos

La gestión de las operaciones y comunicaciones tiene como fin garantizar que se cumplan los requisitos de seguridad de la información, teniendo en cuenta el funcionamiento de los recursos computacionales y las comunicaciones en la organización.

Por lo tanto, esta gestión incluye el tratamiento de los servicios subcontratados, la protección contra códigos maliciosos, la política de copias, la seguridad de redes, medios y transferencia de software e información, además de la vigilancia global de todos los aspectos de las operaciones y las comunicaciones dentro de la organización.

6.2 Procedimientos y responsabilidades operacionales

Con respecto a los procedimientos y las responsabilidades operativas, algunas prácticas son consideradas esenciales, con el objetivo de garantizar la adecuación de las operaciones a los requisitos de seguridad de información de la organización. Esas prácticas se detallan a continuación:

- Documentar los procedimientos operacionales de manera formal y flexible (en el sentido de permitir cambios cuando sea necesario y autorizado) englobando el tratamiento de las operaciones de mantenimiento, manipulación de errores, y otras condiciones adversas, los contratos de soporte, los procedimientos de recuperación, generación de copias de seguridad, entre otros.
- Controlar cambios operativos, definiendo las responsabilidades de gestión y, cuando sea posible, integrar los procedimientos de control de cambios para las aplicaciones y sistemas operativos. Es importante mantener un registro de auditoría cuando se realizan cambios.
- Establecer procedimientos para la gestión de incidentes, como acción para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad.
- Separar las responsabilidades, con el fin de reducir los riesgos de mal uso de los sistemas, por ejemplo, impidiendo que una única persona pueda acceder, modificar o utilizar los activos sin autorización. Por lo tanto, es importante separar la gestión de ciertas responsabilidades o áreas de responsabilidad para que las posibilidades de modificaciones no autorizadas se reduzcan.
- Separar instalaciones de desarrollo, pruebas y operación, estableciendo un nivel de separación necesaria para evitar problemas de funcionamiento, sobre todo en términos de acceso o modificaciones no autorizadas. Por ejemplo, las reglas para cambiar el estado de un software (de desarrollo a producción) deben ser definidas y documentadas.

Ejemplo: el tratamiento de las responsabilidades operativas:

- "Los usuarios que utilicen los sistemas de las TI de la organización deben firmar un contrato de responsabilidad antes de acceder a ellos. La firma del contrato significa que el usuario entiende y está de acuerdo con las políticas y normas de seguridad y tiene conocimientos sobre la legislación vigente y aplicable en los casos de incumplimiento".

En el ejemplo, se presenta una regla que hace referencia a contrato de responsabilidad que determina, a su vez, todas las responsabilidades de los usuarios relacionadas con el correcto funcionamiento de los sistemas de las TI de la organización, de acuerdo con las políticas y normas de seguridad de la información vigentes, y también determina la aplicación de la Ley en caso de incumplimiento.

La planeación anticipada es importante para garantizar los recursos necesarios para los sistemas, lo que facilita su adopción en la organización. En este contexto, son importantes la planificación de capacidad y un proceso adecuado de homologación.

En la planeación de capacidad, se atienden las demandas por capacidades futuras, con el fin de proporcionar el poder de procesamiento y almacenamiento adecuados a los requisitos de la organización. También es saludable la preocupación por las tendencias con respecto a las aplicaciones y sistemas de información, entre otros aspectos influyentes en el contexto.

En cuanto a la homologación, es importante determinar de antemano los criterios de aprobación y aceptación, y las pruebas adecuadas para los sistemas. Algunos criterios relevantes son: rendimiento, capacidad de procesamiento, recuperación de errores, planes de contingencia y medidas de seguridad adoptadas. En particular, todos los criterios y supuestos considerados para la aprobación deben ser definidos, acordados, documentados y probados.

Ejercicio de refuerzo - procedimientos y responsabilidades operacionales

» Explique la práctica de la segregación de responsabilidades.
» Explique cómo debe ser la planificación de capacidad.

6.3 Protección contra software malicioso

Hay varias posibilidades, tales como virus, troyanos, bombas lógicas, etc. La protección debe estar basada en crear conciencia sobre la seguridad, control de acceso y el cambio. Algunas de las prácticas son:

» Controlar la conformidad de las licencias de software.
» Controlar los riesgos asociados a los archivos y software obtenidos a través de la red.
» Instalar y actualizar periódicamente los antivirus.

Dada la variedad de *malware* existente actualmente, es de suma importancia asegurar controles en relación con los recursos de procesamiento de información y software en las organizaciones. Algunas prácticas pueden aplicarse al contexto, como el uso de software para detectar *malware*, antivirus, control estricto de acceso, un control adecuado de cambios, prohibición del uso de software no autorizado y precauciones con archivos y software obtenidos a través de la red.

También se recomiendan algunas comprobaciones: revisar la presencia de código malicioso en archivos y medios ópticos o electrónicos transmitidos a través de la red, recibidos por correo electrónico, páginas web, tanto en los servidores como en las estaciones de trabajo de los funcionarios de la organización.

Reglas para la protección contra códigos maliciosos:

- No abrir los archivos o ejecutar programas adjuntos a mensajes de correo electrónico sin verificar primero con un programa de detección de virus.
- No utilizar formatos ejecutables en los archivos comprimidos, dado que este formato facilita la propagación del virus.
- Usar software licenciado para su uso por la organización, de acuerdo con las disposiciones específicas establecidas en el contrato.

En el ejemplo, se presentan las normas que rigen para cualquier organización, con el objetivo de establecer recomendaciones para la protección contra códigos maliciosos y que puedan provocar incidentes de seguridad. En particular, también se presenta una regla para la instalación de programas, como una medida preventiva para la instalación de software malicioso.

Ejercicio de refuerzo - protección contra software malicioso

- ¿Cuáles son algunas de las prácticas que se pueden aplicar para la protección contra software malicioso? De ejemplos.
- Cite algunas reglas que se pueden aplicar en su organización.

6.4 Las copias de seguridad

Las copias de seguridad (*backups*) representan los controles destinados a garantizar la integridad y disponibilidad de los activos. En este contexto, se debe prestar atención no sólo a la generación de copias, sino también a que la generación se haga con regularidad y sea probada, y que la recuperación se lleve a cabo en un tiempo aceptable.

Se recomiendan algunas prácticas para el tratamiento de las copias de seguridad:

- Registrar y documentar los procedimientos de recuperación a partir de copias de seguridad;
- Definir el modo (ya sea completa o incremental) y la frecuencia de generación de las copias, de acuerdo a la criticidad de los activos y a los requerimientos del negocio y de seguridad de la organización;
- Almacenar las copias en lugares remotos o suficientemente distantes para no ser afectados por los desastres ocurridos en la ubicación específica de la organización;
- Identificación de los niveles adecuados de protección física y ambiental de las copias;
- Aplicar pruebas regulares a los medios utilizados en la generación de copias;
- Probar regularmente los procedimientos de recuperación.

Las copias de respaldo deben mantener duplicados de la información esencial para el negocio y deben ser probadas con regularidad para cumplir con los requisitos de los planes de continuidad del negocio.

Ejercicio de refuerzo - copias de seguridad

- ¿Cuáles son los objetivos de las copias de seguridad?
- ¿Cuáles son algunas de las prácticas que se pueden aplicar en su organización?

6.5 Políticas de copias de seguridad

Mantener las copias de seguridad completas y actualizadas son una actividad importante en los planes de contingencia de la organización, dado que permiten comparar los sistemas y datos actuales con las copias de seguridad en caso de problemas y luego hacer la recuperación adecuada.

La política de seguridad se determina de acuerdo con el grado de importancia de los sistemas y de la información para el negocio de la organización; por eso, establece los procedimientos, las pruebas y la infraestructura necesaria para la protección de copia de seguridad con el fin de garantizar la continuidad del negocio en caso de desastre o incidente de seguridad.

En términos de estrategias, se puede determinar copias de seguridad completas o incrementales (en uno o más niveles) con frecuencia variable en función de la importancia del sistema o de la información en cuestión.

Ejemplos

Reglas para el tratamiento de las copias de seguridad:

- A cada empleado le corresponde realizar regularmente, una copia de seguridad de sus datos.
- Mantenga un registro de las copias creadas de seguridad.
- Guarde las copias de seguridad en un lugar seguro y diferente de donde se encuentra la información original.
- En el ejemplo, se presentan las reglas aplicables a cualquier organización, con el objetivo de establecer las prácticas relacionadas a la generación y mantenimiento de copias de seguridad.

Ejercicio de refuerzo - políticas de copias de seguridad

- ¿Cómo debe ser determinada la política de copias de seguridad?

6.6 El tratamiento de los medios y documentos

Los medios magnéticos (discos, cintas, DVD/CD, etc.) y la documentación deben estar protegidos de las amenazas por interrupción, interceptación, modificación y fabricación. Por lo tanto, algunas prácticas son aplicables:

- Tener en cuenta la clasificación de la información antes de establecer los procedimientos y medidas de seguridad para su procesamiento, almacenamiento y transmisión;
- Controlar el acceso al contenido de medios y documentos;
- Desechar de forma segura medios y documentos que ya no son útiles, con base en los procedimientos formales. Por ejemplo, usando incineración o trituración;
- Para el trasporte de medios se deben establecer reglas claras en cuanto a los transportadores, el embalaje, los modos de entrega (en mano, por correo, etc.).

Ejercicio de refuerzo - tratamiento de medios y documentos

- ¿Cuáles son las dos prácticas que se deben adoptar en su organización para el tratamiento de los medios y documentos?

6.7 Gestión de la seguridad de la red

Es importante utilizar medidas de seguridad de red adecuadas en las organizaciones, de acuerdo con la política de seguridad y los requisitos legales, contractuales y reglamentarios. Para ello, se recomienda tener en cuenta las responsabilidades operativas de la red y los procedimientos necesarios (incluyendo el acceso remoto) para coordinar su gestión.

Se recomiendan algunas prácticas para este contexto:

- Separar las responsabilidades operativas de la red de otras operaciones;
- Identificar los requisitos de seguridad, niveles de servicio y los requisitos de gerencia de servicios de red para la organización (ya sea interno o subcontratado). Los servicios de red incluyen,

por ejemplo, las conexiones y el suministro de soluciones de seguridad tal como *firewalls*;
» Determinar responsabilidades y los procedimientos adecuados para la gestión de la red y de los equipos remotos;
» Aplicar las medidas de seguridad que garanticen la confidencialidad e integridad de los datos en tráfico y la disponibilidad de los recursos involucrados en las comunicaciones.

Ejercicio de refuerzo - gestión de seguridad de la red

» Cite dos prácticas que se deben adoptar en su organización para la gestión de seguridad de la red

6.8 La transferencia de información y el software

Se debe garantizar la seguridad en cualquier modalidad de transferencia (interna o entre la organización y terceros) de la información y software. Es de destacar que, por el contexto, estos recursos se consideran relevantes: e-mail, voz, video, comercio electrónico, descargas de software y la compra a los proveedores, por ejemplo.

En particular, la transferencia de información y software entre organizaciones debe llevarse a cabo bajo las reglas de una política formal específica (o acuerdos específicos) y los requisitos legales, contractuales y reglamentarios vigentes.

En general, las siguientes prácticas pueden ser consideradas:

» Protección contra software malicioso;
» Definir claramente las reglas para el uso de los recursos electrónicos, como el correo electrónico y los servicios web. Por ejemplo, la restricción de las retransmisiones de mensajes de correo electrónico a direcciones externas de correo electrónico;
» Establecer procedimientos para el uso seguro de la comunicación inalámbrica (*wireless*);
» Garantizar que los recursos utilizados en la transferencia de información y de software cumplen con la legislación vigente;
» Declarar claramente las responsabilidades de las partes involucradas en los casos de ocurrencia de incidentes de seguridad.

6.9 Monitoreo

El monitoreo de las operaciones y las comunicaciones debe ser una tarea regular y con el apoyo de los líderes de la organización, con el fin de garantizar la adecuada seguridad de la información con relación a los recursos operativos y de comunicación disponibles, y de acuerdo a las necesidades que surgen tras el análisis/evaluación de riesgos de seguridad de la organización. También se recomienda que todos los eventos relacionados con el monitoreo se registren correctamente a través de los *logs* de funcionamiento, de fallas y de auditoría, por lo menos.

En particular, las actividades de vigilancia y el registro se llevarán a cabo de conformidad con la legislación vigente. Todos los *logs* deben ser protegidos contra el acceso no autorizado.

Las siguientes prácticas pueden ser adoptadas para el mantenimiento adecuado de los registros:

- El *log* de operaciones debe mantener información tal como las actividades de los operadores y administradores de sistemas, el horario de inicialización y cierre de sistemas, errores y acciones correctivas implementadas, por ejemplo;
- El *log* de fallas debe registrar las fallas y las acciones correctivas tomadas. En particular, es importante que existan reglas claras para el manejo de reportes de fallas en la organización

Los *logs* de auditoría se deben mantener con el fin de registrar las actividades del usuario, los problemas de seguridad, los cambios de configuración de los sistemas, todos los accesos realizados, por un período adecuado de tiempo para las actividades de auditoría y supervisión .

Ejemplos de procedimientos con los *logs*:

- "No se permite el acceso no autorizado al correo electrónico de terceros. Los intentos de acceso deben ser registrados en *log*, incluyendo los causados por los administradores del sistema. "
- "Debería ser posible reconstruir todas las actividades de los usuarios a partir de los *logs*. Los procedimientos utilizados para dicha supervisión deben tener en cuenta los mecanismos claros y divulgados de responsabilidad en los medios de comunicación internos de la organización. "

Se ejemplifican algunos procedimientos relevantes a considerar en cuanto a la generación de *logs* en la organización. Los ejemplos pueden ser considerados para organizaciones reales y su objetivo es permitir el monitoreo de las operaciones y actividades de los usuarios en particular.

Capítulo

07

Seguridad de acceso y del entorno

Objetivos

Describir los procedimientos y responsabilidades y seleccionar y aplicar los controles y procedimientos de seguridad de acceso y del entorno.

Conceptos

Política de control de acceso, controles de acceso lógico y físico, control del entorno y seguridad en recursos humanos

Ejercicio de nivelación - seguridad de acceso y del entorno

» ¿Qué entiende por acceso físico?
» ¿Qué entiende por acceso lógico?

7.1 Política de control de acceso

La política de control de acceso debe ser definida y documentada por las organizaciones para garantizar las medidas y procedimientos de seguridad adecuados a los recursos físicos y lógicos, de conformidad con los requisitos del negocio. Por lo tanto, la política de control de acceso, al menos, debería tener en cuenta:

» Información manejada por las aplicaciones de negocio y los riesgos inherentes que hay;
» La clasificación de la información;
» La legislación, los requisitos reglamentarios y contractuales vigentes y pertinentes a la protección de acceso
» Requisitos para la autorización formal de las solicitudes de acceso y remoción de derechos;
» Requisitos para la comprobación periódica de los controles de acceso.

Tenga en cuenta que la política debe contemplar, en conjunto, los controles de acceso lógico y físico.

Clasificación de la información:

Proceso para la definición de la sensibilidad de la información y quién tiene acceso a esta información, lo que permite definir los niveles de acceso y criterios que garanticen la seguridad de la información.

Ejercicio de refuerzo - políticas de control de acceso

» ¿Qué se debe tener en cuenta en la política de control de acceso?

7.2 Controles de acceso lógico

En términos de control de acceso lógico, se verán a continuación sub-temas que abordan las principales preocupaciones y mejores prácticas para el contexto, además presenta los aspectos claves para el control de acceso lógico conforme a los requisitos de seguridad global y de negocios de las organizaciones.

El control de acceso lógico comprende un conjunto de medidas y procedimientos adoptados por la organización o intrínsecos al software y sistemas utilizados, y tiene como objetivo proteger los recursos informáticos y la información, para asegurar:

» Que sólo los usuarios autorizados tengan acceso a los recursos y que estos recursos son los realmente necesarios para el desempeño de sus actividades;
» Que el acceso a los recursos críticos sea restringido y supervisado adecuadamente. En otras palabras, se puede considerar que el control de acceso lógico es un proceso que utiliza las medidas preventivas y procedimientos específicos para que los usuarios o procesos accedan a los recursos de modo adecuado.
» Cuando se trata de control de acceso, primero se deben identificar los recursos a proteger. Éstos son algunos típicamente identificados en las organizaciones: aplicaciones (código fuente y objeto), archivos de datos y contraseñas, redes, utilidades, sistemas operativos, archivos de *log*, entre otros.

Recuerde que capacitar a los usuarios es una tarea importante para garantizar la eficacia de las medidas y procedimientos adoptados para el control de acceso. Por lo tanto, una buena práctica es que los usuarios se mantengan informados sobre sus responsabilidades con el mantenimiento de los controles de acceso de la organización.

Estudie la sección 11 (Control de accesos) de la norma ISO / IEC 27002:2007.

Las funciones directamente relacionadas con el control de acceso lógico son: identificación y autenticación, para usuarios y los procesos, y atribuciones, gestión y monitoreo de los derechos de acceso o privilegios que indican exactamente el grado de autorización de acceso:

- **Identificación:** cada usuario/proceso que puede acceder a los recursos computacionales se debe identificar exclusivamente en el ambiente, por ejemplo, vía *login*, para permitir el control de acciones mediante *logs*.
- **Autenticación:** más allá de la identificación, el usuario deberá proporcionar alguna información complementaria para probar que esta es su verdadera identidad. Por ejemplo, un usuario realiza un inicio de sesión en una estación de trabajo debe informar su identificación (*login*) y contraseña, este es el autenticador que permite que el sistema compruebe si la identidad del usuario es correcta. Por lo tanto, la autenticación tiene como objetivo proporcionar una forma de verificación de la identidad de los usuarios/procesos antes de que obtengan acceso a los recursos. Por lo tanto, hay básicamente tres formas posibles: prueba por características (físicas), prueba por posesión y pruebas de conocimiento. Por ejemplo, usando reconocimiento facial o de voz, *smart cards* y contraseñas (*token*), respectivamente.
- **Atribuciones:** la asignación de derechos y permisos de acceso se puede determinar en dos aspectos: lo que un usuario/proceso puede hacer o lo qué se puede hacer con un recurso determinado. En la primera posibilidad, cada usuario o recurso recibe un permiso que, a su vez, define todos los derechos de acceso a otros recursos. En la segunda, se utilizan listas de control de acceso (*Access Control List, ACL*) para cada recurso, definiendo así los derechos de acceso de otros recursos o usuarios sobre el recurso asociado con estas listas.
- **Monitoreo:** se puede hacer mediante la verificación de *logs*, registros de auditoría, los mecanismos de detección de intrusos, entre otros, que pueden servir para tomar decisiones con res-

pecto a las medidas correctivas adecuadas en caso de incidentes de seguridad.
- **Gestión:** responsable de aplicar las medidas adecuadas a los riesgos inherentes a controles de acceso lógico inadecuadas, de acuerdo con las determinaciones dispuestas en controles de políticas de seguridad.

La gestión de los controles de acceso lógico debe implementar medidas que reduzcan los riesgos, observando, por lo tanto, algunas consideraciones definidas en la política de seguridad de la organización, a saber:

- Clasificación de los sistemas e información;
- Necesidades de obtención de acceso a sistemas y datos;
- Responsabilidades de los usuarios;
- Los valores de los activos;
- Otra información relevante para un adecuado control de acceso lógico.

En particular, cuando se trata de la gestión de control de acceso lógico, con respecto a la autorización, es importante tener en cuenta el mantenimiento adecuado de los derechos de acceso a los nuevos recursos y el uso de dispositivos móviles (*notebooks*, agendas electrónicas, teléfonos inteligentes, etc.) según su riesgo inherente.

Los ejemplos de las recomendaciones para el uso de contraseñas en la gestión de los controles de acceso lógico son:

- "Es el deber de la gestión de la seguridad deshabilitar las cuentas inactivas y sin contraseñas o con contraseñas estandarizadas."
- "La contraseña inicial de usuarios se debe generar de modo que ya esté caducada, obligando a la entrada de una nueva contraseña en el primer inicio de sesión."
- "Las cuentas de usuario se deben bloquear después de un número de intentos de acceso sin éxito."

Estos son ejemplos de las recomendaciones para los procesos de autenticación basados en contraseñas que se pueden utilizar en las organizaciones reales.

Se recomienda guiar a los usuarios para elegir contraseñas más seguras, evitar el uso de contraseñas demasiado cortas o demasiado largas (es recomendable utilizar ocho caracteres), lo que puede causar efectos secundarios tales como escribir las contraseñas en papel, evitando por otra parte, el uso de la misma contraseña para acceder a sistemas/

recursos diferentes. Es interesante, también, el uso de generadores de contraseña aleatoria, aumentando la confiabilidad de los sistemas de autenticación.

Para obtener información sobre las mejores prácticas en el uso de contraseñas, consulte:
https://security.web.cern.ch/security/recommendations/en/passwords.shtml
http://www.csirt.pop-mg.rnp.br/docs/senhas.pdf

Para el manejo adecuado de los controles de acceso lógico en una organización, se recomiendan algunas de las mejores prácticas:

- Asignar derechos de acceso a los usuarios, de acuerdo con las necesidades reales de su trabajo/cargo;
- Revisar las listas de control de acceso y capacidades de forma regular;
- Proporcionar cuentas de usuario sólo a las personas autorizadas;
- Almacenar contraseñas encriptadas;
- Mantener y analizar los *logs* y los registros de auditoría.

Ejercicio de refuerzo - controles de acceso lógico

- ¿Qué funciones están directamente relacionadas con el control de acceso lógico?
- ¿Qué se debe considerar al tratar la gestión de control de acceso lógico con respecto a la autorización?
- Nombre dos buenas prácticas para la gestión de los controles de acceso lógico de su organización.

7.3 Controles de acceso físico

Se verán, a continuación, las principales preocupaciones y las mejores prácticas para el control de acceso físico, con la presentación de los aspectos fundamentales y las influencias provenientes de las exigencias de seguridad global y de negocios de la organización.

Los controles de acceso físico están destinados a poner en práctica medidas preventivas para proteger a los equipos, documentación, suministros e información contra el acceso no autorizado, pérdidas, etc. Por lo tanto, estos controles sirven como una barrera de seguridad adicional para el control de acceso lógico.

También se debe considerar el uso de las áreas protegidas y los perímetros de seguridad. En las áreas protegidas (con estricto control de acceso), se recomienda el tratamiento de la información crítica para el negocio de la organización. Los perímetros de seguridad protegen las áreas que tienen instalaciones de procesamiento, por ejemplo, un control de acceso con registro y supervisión efectiva.

En cuanto a los controles de acceso físico, hay dos categorías, a saber:

- **Controles administrativos:** incluyen las medidas y los procedimientos administrativos para la protección física de la organización. En términos prácticos, se recomienda, en este contexto, la aplicación de formas de identificación única para personal y para visitantes, e incluso las categorías de los funcionarios; exigir la devolución de los activos de la organización en caso de despido de los empleados; controlar la entrada/salida visitantes; exigir "escritorio limpio" y organizado, entre otros;
- **Controles explícitos:** implementados mediante el uso de cerraduras, candados, cámaras de video, alarmas y guardias de seguridad, por ejemplo.

Ejemplo de recomendación para el control de acceso físico a los equipos:

- "El acceso a equipos específico de hardware debe limitarse a personal competente, con uso registrado y basado en las necesidades de la organización."

En este ejemplo, se presenta una recomendación para el control de acceso físico en las organizaciones, y se pueden incluir en organizaciones reales como elemento de la política de control de acceso y de la política de seguridad.

La gestión de los controles de acceso físico debe tratar de averiguar los riesgos potenciales y los impactos causados por los incidentes originados por fallas de seguridad físicas, aplicando medidas adecuadas para la organización.

Tenga en cuenta que, como se dijo anteriormente, las medidas y los procedimientos de los controles de acceso físico deben ser incluidos en la política de control de acceso, apoyando la política de seguridad de la información de la organización y, en consecuencia, dichos documentos en conjunto apoyan la gestión de los controles de acceso físico.

Entre las mejores prácticas para el adecuado control de acceso físico (y su gestión), se encuentran:

- Use técnicas de identificación visibles;
- Exigencia de la devolución de los activos de la organización cuando el empleado es despedido o separado de sus funciones;
- Supervisar la entrada y salida de visitantes, registrando la fecha, el tiempo de permanencia y el lugar visitado (sector, departamento, etc.)
- Determinar la vigilancia permanente (7 x 24) en la organización;
- Revisar y actualizar periódicamente los derechos de acceso;
- Fomentar la política de escritorio limpio, entre otros.

Ejercicio de refuerzo - controles de acceso físico

- ¿Cuál es el propósito de control de acceso físico?
- ¿Cuáles son los controles explícitos y controles administrativos?
- Nombre dos buenas prácticas para la gestión de los controles de acceso físicos de su organización.

7.4 Controles ambientales

En términos de control ambiental, se presentan algunas de las prácticas específicas para reducir los riesgos asociados a amenazas en el entorno de las organizaciones, de acuerdo con los requisitos del negocio y la seguridad global.

Los controles de ambiente tienen por objeto proteger a la organización en términos, específicamente, de la disponibilidad y la integridad de sus recursos, es decir, contra los desastres naturales y las fallas en el suministro o descargas de energía eléctrica, por ejemplo.

Dependiendo de la amenaza, se pueden establecer las medidas preventivas y/o correctivas. Se presentarán las siguientes mejores prácticas para garantizar los controles ambientales apropiados.

A continuación tenemos una lista de las principales amenazas y las medidas de control aplicadas:

- **Los incendios:** se aconseja el uso de dispositivos de detección de humo o calor, instalación de pararrayos, la adopción de políticas de ambientes libres de humo, la disposición de un número suficiente de extintores de incendios, la instalación de los sistemas automáticos de extinción de incendios, la verificación regular de todos los dispositivos contra incendios y el entrenamiento de los empleados en cuanto a su uso;
- **Las fallas en la electricidad y las descargas eléctricas naturales:** se recomienda el uso de estabilizadores, UPS, generadores alternos de energía, la instalación de pararrayos, apagado del equipo en situaciones de fuertes tormentas;
- **Las amenazas relacionadas con el agua:** es pertinente la instalación de los equipos en lugares con baja susceptibilidad al agua, mantenimiento adecuado de los tejados, red de alcantarillado y equipos de aire acondicionado;
- **Temperatura y ventilación:** deben ser considerados en este caso, el cuidado de los canales de ventilación, la circulación de aire, dispositivos que ayudan en el control de la temperatura y la ventilación del ambiente y el mantenimiento periódico de este equipo

A continuación se presenta una lista de las mejores prácticas para garantizar el control adecuado del entorno en las organizaciones:

- Planificar la ubicación de muebles y equipos, facilitando la circulación de las personas;
- Mantener la limpieza y conservación del ambiente;
- Implementar sistemas automáticos de extinción de incendios;
- Instalar los dispositivos que minimicen los efectos de las fallas en suministro de energía eléctrica;
- El mantenimiento adecuado de potenciales focos de problemas con agua;
- Inspeccionar regularmente todos los dispositivos directamente relacionados con la conservación de la seguridad del ambiente.

Ejercicio de refuerzo – controles del entorno

» ¿Cuál es el propósito de los controles del entorno?
» Nombre dos buenas prácticas recomendadas para la gestión de los controles de acceso físicos en su organización

7.5 Seguridad de recursos humanos

En esta sección serán presentados algunos de los principales aspectos de la seguridad de la información en las organizaciones; la seguridad de los recursos humanos, el cual, a su vez, es uno de los pilares para la seguridad de la información adecuada y concientizada en términos de los posibles errores humanos. Será vista en algunas prácticas y preocupaciones para el tratamiento de las personas, desde la selección, considerando también la capacitación en términos de seguridad de la información.

Estudie la sección 8 (recursos humanos de seguridad) de la norma ISO/IEC 27002:2007.

La selección de los candidatos deberá ser estricta en función, principalmente del cargo deseado y su criticidad para el negocio. Tenga en cuenta que el "candidato" puede representar un posible empleado, un empleado que busca cambiar de cargo o incluso un prestador de servicios.

Durante la selección de las personas, la organización debe dejar claro las responsabilidades y funciones de los candidatos en caso de contratarlos, frente a la seguridad de la información, a través de la presentación de una descripción detallada y de los términos y condiciones del contrato.

Por lo tanto, es importante destacar, en los documentos a ser firmados por el contratista, requisitos como actuar de acuerdo con la política de seguridad de la información y notificar a los superiores respecto a los eventos adversos que pueden caracterizar riesgos de seguridad de la organización.

La selección en sí, como se dijo antes, debe ser lo suficientemente estricta como para contemplar la verificación de referencias personales satisfactorias; confirmación de las calificaciones académicas y profesionales, y también puede considerar verificaciones financieras (crédito) y de registros penales. Es de destacar también que pueden ser relevantes, dependiendo de la situación, una selección estricta de proveedores y contratistas.

Los términos y condiciones deben estar claramente establecidos en el contrato, por lo que éste se firma indicando que el contratista está de acuerdo con sus responsabilidades relacionadas con la seguridad de la información de la organización (incluyendo las responsabilidades legales). En este contexto, también es conveniente la orientación para que se siga un código de conducta y se firme un acuerdo de confidencialidad antes de facilitar el acceso al contratista.

El acuerdo de confidencialidad debe incluir requisitos para la protección de la información confidencial, teniendo en cuenta la legislación vigente. En particular, el contenido debe comprender por lo menos una definición de la información a proteger, la duración del acuerdo, las responsabilidades y las acciones de los involucrados para evitar la divulgación no autorizada, el alcance de los derechos de los empleados en el uso de la información, los derechos de auditoría y monitoreo, y las acciones específicas en caso de violaciones al acuerdo.

Al cancelar o cambiar el contrato de un empleado (o tercero), es importante que la organización facilite los medios adecuados para un proceso ordenado y coordinado.

En este contexto, algunas prácticas son aplicables:

- Tras la terminación de una función, una comunicación debe informar acerca de los requisitos de seguridad y las responsabilidades legales exigidas;
- Devolución de activos, tales como equipos, documentos, software, computadores portátiles, tarjetas de crédito, tarjetas de acceso, carnets, etc.;
- Retire los derechos de acceso a la información y recursos. En caso de cambio de cargo, se deben revisar los derechos, con

el fin de no permitir accesos que no han sido aprobados para la nueva función. Si, por ejemplo, el empleado con actividades finalizadas en la organización tiene conocimientos acerca de las contraseñas de las cuentas que se mantienen activas después de su partida, estas deben ser cambiadas.

Ejercicio de refuerzo - seguridad recursos humanos

» ¿Durante el proceso de desvinculación de la organización de un colaborador por finalización del contrato, qué se debe hacer?

Si los empleados o terceros no están realmente conscientes en cuanto a sus responsabilidades y obligaciones con la seguridad de la información de la organización, pueden considerarse en sí mismos como riesgos, y pueden causar impactos al negocio.

Por lo tanto, se debe promover entrenamiento regular, conferencias y actividades de divulgación de directrices para la seguridad de la información a todas las personas, de modo que conozcan los procedimientos de seguridad, que hagan un uso adecuado de los recursos, servicios ofrecidos e información.

En los procesos de capacitación para la seguridad de la información, es importante concientizar a las personas en términos de riesgos, e informarles a quién deben reportar eventos adversos y como buscar orientación.

A través de iniciativas de educación en seguridad de la información, es posible minimizar los riesgos, dado que las personas son sensibilizadas a seguir las reglas de seguridad de la información en su vida cotidiana.

Ejemplo de recomendación para la conducta de las personas ante el uso de recursos de información crítica:

» "La organización se reserva el derecho de revocar los privilegios de usuario de cualquier sistema y en cualquier momento debido a un comportamiento ofensivo o dañino o incluso que afecte la capacidad de otras personas para realizar correctamente sus funciones.

En este ejemplo se presenta una recomendación para el tratamiento de las personas en las organizaciones, en particular las normas explícitas para su conducta hacia los negocios y la manipulación de los recursos y la información crítica. Esta recomendación también se puede aplicar para una seguridad eficiente del recurso humano.

Capítulo

08

Seguridad organizacional

Objetivos

Describir los procedimientos y responsabilidades, y seleccionar y aplicar controles de seguridad organizacional.

Conceptos

Infraestructura organizacional para la seguridad de la información, el tratamiento de los activos y la seguridad de la información de terceros.

Ejercicio de nivelación - seguridad organizacional

» ¿Qué se entiende por seguridad organizacional?
» ¿Cómo se hace la seguridad organizacional en su institución?

8.1 Infraestructura organizacional para la seguridad de la información

En esta sección se presentarán los temas relevantes para el establecimiento de una infraestructura de apoyo a la seguridad de la información en las organizaciones. En particular, se tratará la importancia de la infraestructura, la relevancia de la asignación de responsabilidades y aspectos relacionados con la coordinación.

8.1.1 Importancia de la infraestructura

Para garantizar la seguridad de la información de una organización en particular, se debe prestar atención a la necesidad de establecer una infraestructura que fomente la gestión. Inicialmente, es válido definir una estructura de gestión propia para el control de la implementación de seguridad de la información.

En particular, si fuere el caso, es relevante la contratación de una consultoría especializada con el propósito de elaborarla e implantarla en la organización.

8.1.2 Asignación de responsabilidades

Asignar responsabilidades se considera una actividad crucial para la seguridad de la información y se debe realizar de acuerdo con la política de seguridad de la información de la organización.

Los funcionarios (o personas en ciertas posiciones) que tengan responsabilidades definidas formalmente en la política de seguridad pueden delegar directamente las actividades relacionadas con la seguridad de la información, sin embargo, no se eximen de su responsabilidad. Por lo tanto, es relevante que en el caso de delegación, los funcionarios que delegan la actividad evalúen si ésta se lleva a cabo conforme a la política de seguridad, la legislación y las normas vigentes.

Para cada activo y procedimiento de seguridad de la información, es importante asignar responsabilidades a un funcionario (o cargo). En otras palabras, el funcionario (o cargo) debe realizar la gestión del activo o del procedimiento según se determine en la política de seguridad.

Dependiendo del tamaño y de las vulnerabilidades de la organización, se puede establecer el cargo de gestor de seguridad de la información, que es responsable en primera instancia, de la seguridad general de la organización y también ayuda en el desarrollo de la política de seguridad y define la estrategia para su divulgación, exigiendo el cumplimiento por parte de todos. El gestor, debe estar siempre actualizado sobre los problemas, riesgos y soluciones de seguridad; seleccionar los mecanismos de seguridad más adecuados para los problemas de seguridad específicos de la organización; y verificar la adecuación de la política de seguridad, mecanismos y procedimientos de seguridad de la información que se adopten.

Ejercicio de refuerzo - asignación de responsabilidades

- ¿Qué tareas deben asignarse al gestor de seguridad de la información?
- ¿Por qué la asignación de responsabilidades es fundamental para la seguridad de la información?

8.1.3 Coordinación de la seguridad de la información

Para la efectividad de la seguridad de la información en una organización, sus líderes deben reunir un equipo multidisciplinario (directivos y funcionarios de varios departamentos, por ejemplo) para coordinar las actividades necesarias. Si es necesario, también se puede establecer un comité específico. En particular, se recomienda que actúe para coordinar las siguientes actividades:

- Evaluar y aprobar las metodologías y procedimientos para la seguridad de la información;
- Controlar todos los procedimientos, con el fin de garantizar el cumplimiento de la política de seguridad de la organización;
- Coordinar la implantación de los controles de seguridad de la información, tales como las medidas contra el acceso no autorizado;
- Divulgar adecuadamente a toda la organización los procedimientos, los controles y la política de seguridad. Recuerde siempre que la concientización de las personas puede ser considerada tan relevante como el uso de otros mecanismos de seguridad basados en la tecnología.

Ejercicio de refuerzo - coordinación de la seguridad de la información

- ¿En qué actividades debe actuar el comité?

8.2 Tratamiento de los activos

Teniendo en cuenta que los activos son elementos esenciales para el negocio de las organizaciones, esta sección presenta los aspectos principales a tener en cuenta. Se presentarán las preocupaciones sobre la protección de los activos y de los procedimientos recomendados, aplicados a la gestión de activos y recuperación de desastres: inventario y designación de propietario para cada activo de la organización.

8.2.1 Protección de activos

Los activos de la organización son elementos importantes para el negocio, por lo que una protección adecuada debe ser establecida y mantenida. Ejemplos:

- Equipos;
- Bases de datos;
- Servicios de iluminación;
- Acuerdos;
- Procedimientos de soporte técnico;
- Los registros de auditoría;
- Aplicativos;
- Sistemas de información;
- Personas;
- Imagen comercial de la organización.

Para tal protección se recomiendan dos procedimientos: hacer un inventario de los activos y asignar a cada uno un propietario, responsable por el mantenimiento de su seguridad.

A continuación se presentará más detalles acerca de cada procedimiento.

Ejercicio de refuerzo - protección de los activos

- ¿Qué son los activos?

8.2.2 Inventario de activos

En el inventario de los activos, se debe estructurar y mantener los activos debidamente identificados. En la identificación, las información relevante por lo general es: el tipo de activos, configuración, su criticidad para el negocio de la organización, la ubicación, la información sobre el tratamiento de *backups* y licencias. En el inventario también se deben identificar el propietario de cada activo y la clasificación de la información, cuando sea apropiado.

En el caso de recuperación de desastres, el inventario de activos es uno de los elementos esenciales para su efectividad. Y, para la gestión del riesgo, el inventario es una premisa.

Ejercicio de refuerzo - inventario de activos

» ¿Qué información debe incluirse en el inventario de los activos?

8.2.3 Propiedad de los activos

El propietario de un activo es el responsable de mantener su seguridad, realizando actividades tales como:

» Garantizar la clasificación adecuada de los activos;
» Definir y analizar, periódicamente, las restricciones de acceso al activo.

Son ejemplos de propietarios de activos el gerente de RRHH (Recursos Humanos) de la organización encargada de documentos específicos y el desarrollador responsable por su estación de trabajo. Es de destacar que, en caso necesario y apropiado, se puede atribuir al gestor de seguridad de la información la responsabilidad por ciertos activos, especialmente aquellos directamente relacionados con la seguridad de la información, tal como la propia política de seguridad.

Este ejemplo proporciona alguna información sobre el activo "base de datos" de una organización. Se puede observar que:

» El tipo considerado es "datos". La clasificación de los activos puede variar de una organización a otra, pero por lo general se pueden clasificar en hardware, software, datos, documentación, etc.
» La criticidad del activo se considera alto, teniendo en cuenta que los datos son esenciales para el negocio de la organización. Puede asociar la criticidad asignado a las categorías utilizadas en el análisis/evaluación de riesgos para la organización. A modo de ejemplo, los activos pueden ser clasificados como alta, moderada o baja criticidad.
» La ubicación del activo es la sala de servidores en toda la organización, dado que es una base de datos almacenada en una base de datos.
» El tratamiento aplicado al *backup* del activo es incremental y diario. Para todos los activos es relevante indicar la política de copia de seguridad para la gestión de incidentes, en particular. Para efectos de conocimiento, la política puede determinar, de conformidad con el grado de criticidad del activo, el *backup*

completo o incremental y su período (mensual, quincenal, semanal o diario, por ejemplo).

Por último, se asigna el responsable de la seguridad del activo. En este caso, el administrador de la base de datos de la organización.

Ejercicio de refuerzo - propietario del activo

» ¿Cuál es la responsabilidad del propietario del activo?
» Cite las actividades que debe realizar el propietario del activo.

8.3 Seguridad de la información de terceros

Es importante establecer procedimientos apropiados antes de facilitar el acceso por parte de terceros. En este tema, se tratará el por qué del tratamiento diferenciado de los terceros y los posibles riesgos involucrados; cómo tratar con los clientes en relación al mantenimiento de un acuerdo específico para el contexto y los procedimientos recomendados para la gestión de los servicios externalizados.

8.3.1 La razón del tratamiento diferenciado

Se debe considerar un tratamiento diferenciado a los recursos y la información que sean procesados, transmitidos o gestionados por partes externas, por ejemplo organizaciones de servicios, con el fin de permitir dicho acceso de conformidad con la política actual de seguridad de la información de la organización.

Por lo tanto, es importante hacer un análisis de los riesgos potenciales involucrados y las posibles medidas de seguridad adecuadas cuando se trata con partes externas. En particular, las medidas de seguridad y otros criterios específicos en cuanto a seguridad de la información deben ser definidas de común acuerdo entre las partes.

8.3.2 Posibles riesgos

En el tratamiento de la seguridad de la información en relación a terceros, existen riesgos potenciales específicos. Por lo tanto, es importante

analizar y evaluar los riesgos involucrados directamente con el acceso externo, aplicando las medidas de seguridad apropiadas antes de dar el acceso.

Los siguientes son algunos de los aspectos clave a considerar en el contexto:

- Identificar los recursos a los cuales los terceros pueden tener acceso;
- Indicar el tipo de acceso a cada uno de los recursos;
- Conocer el valor y la criticidad de la información a disposición de terceros;
- Aplicar las medidas de seguridad correspondientes a los riesgos para cada información accedida por terceros;
- Considerar las personas que pueden acceder a la información por parte de los terceros;
- Implantar prácticas y procedimientos para el manejo de incidentes de seguridad;
- Considerar los requisitos legales, contractuales y reglamentarios aplicables al contexto.

Ejemplo de normas para el tratamiento de terceros:

- "No se permite la revelación de identificación, autenticación y autorización para uso personal o uso de los recursos autorizados por medio de tales elementos por parte de terceros."
- "No está permitido proporcionar información a terceros acerca de los servicios disponibles en la organización, salvo las de carácter público o con autorización del equipo/gestor competente."

En este ejemplo se presentan reglas para el manejo de la información y servicios por parte de terceros, cuyo objetivo es demostrar la aplicación de procedimientos formales con miras a la seguridad de la información.

Ejercicio de refuerzo - posibles riesgos

- ¿Cuáles aspectos deben considerarse en relación con la seguridad de la información de terceros?

8.3.3 Tratamiento de los clientes

Al tratar con los clientes, la organización debe identificar, por anticipado, todos los requisitos de seguridad directamente relacionados con el acceso externo a los activos y a la información. Por lo tanto, se recomienda:

- Proteger los activos, utilizando mecanismos de seguridad adecuados e indicar las acciones correctivas que deben aplicarse en los casos de peligro;
- Describir en detalle el producto/servicio que va a prestar;
- Considerar las políticas de control de acceso existentes;
- Indicar las responsabilidades legales de la organización y del cliente.

8.3.4 Los acuerdos específicos

En los acuerdos, los requisitos de seguridad deben abordarse con el fin de garantizar el conocimiento y cumplimiento de los mismos por parte de terceros.

En esencia, se recomienda tener en cuenta en los acuerdos lo siguiente:

- La política de seguridad de la información existente;
- El uso de medidas de seguridad para la protección de los activos;
- Entrenamiento y sensibilización de las personas en términos de seguridad de la información y sus responsabilidades;
- Proceso claro de gestión del cambio;
- Políticas de control de acceso;
- Derecho a realizar las auditorías;
- Requisitos para la continuidad de los servicio;
- Responsabilidades legales, contractuales y reglamentarias aplicables.

Inclusive, pueden ser definidos acuerdos de confidencialidad, de manera que los requisitos de seguridad contemplados expresen las necesidades de la organización en cuanto al valor de la información para el negocio. Estos acuerdos protegen la información, al mismo tiempo que determinan las responsabilidades de los participantes en cuanto a la protección, el uso y la difusión de la información de la organización. Por lo tanto, los acuerdos de confidencialidad pueden ser establecidos entre la organización y terceros, y entre la organización y sus empleados.

En las organizaciones donde se externaliza la gestión de seguridad de la información, los acuerdos deberán proporcionar detalles sobre cómo los terceros garantizarán la seguridad acatando las obligaciones legales y los requerimientos del negocio.

8.3.5 Gestión de los servicios de terceros

Los servicios externalizados en una organización deben ser gestionados con el propósito de garantizar su adecuación a los requisitos de seguridad de la información y a los negocios. Por lo tanto, los acuerdos entre la organización y terceros deben ser gestionados y controlados adecuadamente. Prácticas apropiadas:

- Hay que tener en cuenta las medidas de seguridad, niveles de servicio y los requisitos de entrega de servicios en la elaboración de acuerdos de prestación de servicios externalizados. Tales acuerdos deben ser evaluados para verificar que se cumplen los requisitos de seguridad acordados;
- Es importante contar con soluciones técnicas y recursos suficientes para monitorear los acuerdos y los requisitos de seguridad establecidos;
- Se debe monitorear y analizar regularmente los servicios y *logs* proporcionados por terceros;
- Se debe gestionar los cambios en términos de servicios externalizados, teniendo en cuenta las posibles mejoras, actualizaciones de políticas, el establecimiento de nuevos controles de seguridad y uso de las nuevas tecnologías, por ejemplo.

Ejemplo:

- Cláusula contractual: seguridad de la información.

"El contratista se compromete a utilizar programas para la protección y la seguridad de la información que busquen prevenir cualquier acceso no autorizado a sus sistemas, ya sea en relación a los que estén, eventualmente bajo su responsabilidad directa, ya sea a través de un enlace con los demás sistemas del contratante o incluso mediante el uso de e-mail."

Capítulo

09

Gestión de la continuidad del negocio

Objetivos

Identificar los requisitos y organizar la continuidad del negocio; identificar y seleccionar los procedimientos de gestión de incidentes de seguridad.

Conceptos

Gestión de la continuidad del negocio, seguridad de la información y continuidad del negocio, plan de continuidad del negocio y gestión de incidentes.

Ejercicio de nivelación - gestión de la continuidad de negocios

» ¿Qué entiende usted por la continuidad del negocio?
» ¿Cómo es tomada la continuidad del negocio en su institución?

9.1 Continuidad del negocio

En este tema, se verán los aspectos importantes para la continuidad del negocio, así como para su gestión.

Estudie la sección 14: gestión de continuidad del negocio de la norma NTC ISO/IEC 27002:2007.

Hoy en día, las organizaciones dependen de la tecnología y los sistemas computacionales. Por lo tanto, la pérdida de los equipos y la información puede afectar el negocio de la organización, ocasionando pérdidas financieras, de mercado e incluso, dependiendo de la gravedad de las amenazas, provocando su disolución.

En este contexto, es más que necesario la toma de conciencia sobre la necesidad de recuperación de desastres y el plan de contingencia: ambos estratégicos para cumplir con los objetivos de negocio de la organización. Además, también es relevante el plan de continuidad de negocio.

Es de destacar que los líderes de la organización son responsables de revisar los recursos y la información con el fin de identificar la importancia de cada uno para la continuidad del negocio.

El plan de continuidad del negocio es responsabilidad de los líderes de la organización. El equipo de gestión de la seguridad puede ayudar en esta tarea, pero no puede ser responsabilizado por su completa implementación. Esta ayuda puede incluir la creación, mantenimiento, difusión y coordinación del plan de contingencias.

9.2 Gestión de la continuidad del negocio

La gestión de la continuidad del negocio combina la prevención y la recuperación, con el fin de evitar la indisponibilidad de los servicios y actividades del negocio, protegiendo así, los procesos críticos de los impactos causados por fallas o desastres y, en el caso de pérdidas, proporcionar la recuperación de los activos involucrados y restablecer el funcionamiento normal de la organización en un intervalo de tiempo aceptable. En particular, es esencial adoptar la definición de los procesos críticos de la organización y luego integrar la gestión de seguridad de la información de acuerdo con los requisitos de la gestión de la continuidad del negocio.

Algunos ejemplos de los procesos críticos son las operaciones generales, el trato de los funcionarios, los materiales, el transporte y las instalaciones, teniendo en cuenta, para el contexto, sus requisitos específicos de continuidad. Por lo tanto, es importante poner en práctica un plan de continuidad de negocio, con miras a la recuperación de los procesos críticos dentro del rango de tiempo aceptable para el negocio en caso de desastre. Es de destacar que el plan de continuidad del negocio es global para la organización, pero la seguridad de información debe ser considerada como uno de sus componentes.

Para más detalles acerca de la continuidad del negocio, ver las siguientes normas:

- GTC 176:2008-2: 2008 – Guía Técnica Colombiana - Sistema de Gestión de Continuidad del Negocio
- ISO 22301:2012 de *Social security – Business continuity management systems - Requirements.*

Ejercicio de refuerzo - gestión de continuidad de negocio

» ¿Cuál es el propósito de la gestión de la continuidad del negocio?
» ¿Cuáles son los procesos críticos de su institución?

9.3 Seguridad de la información y gestión de la continuidad del negocio

En este tema, se presentarán las principales consideraciones para integrar la seguridad de la información a la gestión de la continuidad del negocio. En particular, se trata el análisis de riesgos y su importancia para ambas.

La seguridad de la información debe ser contemplada como un elemento estratégico a considerar para la continuidad del negocio de una organización. Por lo tanto, cuando se trata de la inclusión de la información de seguridad en el contexto específico, se deben cumplir las siguientes consideraciones:

» La comprensión de los riesgos para la organización en términos de probabilidades e impactos;
» Identificación de los procesos críticos de negocio y los activos directamente relacionados;
» La comprensión de los impactos generados a los negocios por los incidentes de seguridad;
» Identificación de los contratos de seguro establecidos para los activos críticos de la organización;
» Identificación de las medidas preventivas, correctivas e ilustrativas aplicables;
» Identificación de los recursos financieros, de infraestructura, técnicos y ambientales necesarios para la recolección de los requisitos de seguridad;
» Consideración respecto a las medidas relacionadas con la seguridad en los recursos humanos;
» La consideración con respecto a las medidas para garantizar la protección de los recursos de procesamiento;
» La información detallada sobre los requisitos de seguridad de la información a ser incluidos;
» La formalización de las pruebas y del mantenimiento de los planes (de continuidad del negocio y de contingencias, por ejemplo).

Ejemplo de cuestiones a ser consideradas en el plan de continuidad del negocio:

» "La pérdida de la capacidad de protección, procesamiento y recuperación de la información manejada en computadores de la organización, que pueden causar problemas en la realización de sus negocios y no cumpliendo las metas previamente establecidas en el contrato con sus clientes."

El ejemplo presenta un problema que debe abordarse en el plan de continuidad del negocio de las organizaciones.

Ejercicio de refuerzo - seguridad de la información y la gestión de la continuidad del negocio

» ¿De acuerdo con el ambiente de su organización, cuál es la importancia de la comprensión de los impactos generados a los negocios por los incidentes de seguridad?

9.4 Análisis de riesgos y continuidad de negocio

La gestión de la continuidad del negocio debe comenzar por identificar los eventos adversos (identificación de las posibles amenazas), seguido de un análisis de riesgos; no sólo de seguridad, sino también de todos los procesos de negocio, con el fin de determinar el impacto de las interrupciones tanto en relación con la magnitud de los daños causados como en el período de recuperación. Ambas actividades deben llevarse a cabo con la plena participación de los responsables de los procesos y de los recursos de la organización.

Dependiendo de los resultados del análisis de riesgos, un plan específico debe ser desarrollado para determinar la estrategia que se utilizará para lograr la continuidad del negocio. En esta estrategia, hay que determinar, por ejemplo, el intervalo de tiempo aceptable para la recuperación de los sistemas críticos.

Con eso, se dan las condiciones para decidir cómo y dónde invertir en medidas de seguridad, protegiendo los activos y manteniendo las actividades dentro de su mayor normalidad. Una vez desarrollado el plan, que debe ser validado e implementado por los dirigentes de la organización.

Ejercicio de refuerzo - análisis de riesgos y continuidad de negocio

» ¿Cuál es el propósito de realizar un análisis de riesgos en la gestión de la continuidad del negocio?

9.5 Plan de continuidad del negocio

Este tema mostrará las etapas de la implementación de un plan de continuidad de negocio típicamente propuesto para las organizaciones reales, con el fin de tener en cuenta todos los requisitos de seguridad de la información para la continuidad del negocio.

9.5.1 Estructura

La estructura de un plan de continuidad de negocio normalmente debe incluir:

» Responsabilidades individuales necesarias para cada una de las actividades propuestas en el plan;
» Indicación de un gestor específico;
» Las condiciones necesarias para la activación del plan, por ejemplo, la forma de evaluar el efecto adverso, quién notificar, etc.;
» Los procedimientos para garantizar la operación temporal de los procesos y sistemas de negocios, mientras se está ejecutando la recuperación;
» Los procedimientos de emergencia para situaciones en las que hay incidentes que afectan directamente a los negocios;
» Procedimientos de recuperación de procesos y operaciones de negocio en un rango de tiempo aceptable;
» Especificación del calendario de mantenimiento y pruebas a los planes;
» Promoción del entrenamiento en relación con la continuidad del negocio.

9.5.2 Desarrollo e implementación

Durante la planificación de la continuidad del negocio, algunos elementos son determinantes e indican el contenido que se incluirá en el plan, con miras también a la seguridad de la información:

- Identificación de las responsabilidades y los procedimientos para la continuidad del negocio;
- Grado de identificación aceptable de pérdidas de información y servicios;
- La aplicación de los procedimientos de recuperación de las operaciones del negocio y la disponibilidad de información, teniendo en cuenta el marco de tiempo aceptable para restaurar el funcionamiento normal de las operaciones;
- La conciencia de las personas en función de sus responsabilidades y el conocimiento de los procedimientos involucrados;
- Pruebas;
- El mantenimiento regular del plan con el fin de reflejar los cambios significativos en el negocio de la organización.

Es importante tener en cuenta todas las dependencias externas a la organización y los contratos existentes, en particular lo que dice en relación con la legislación específica aplicable. Se recomienda también que se mantenga (actualizados y protegidos) copias del plan de continuidad de negocio en ambientes remotos, como medida de contingencia para situaciones de desastre.

Ejercicio de refuerzo – desarrollo e implementación

- En el entorno de su organización, nombre de tres elementos que son cruciales en la planificación de la continuidad del negocio.

9.5.3 Pruebas

El plan de continuidad del negocio debe probarse periódicamente como una forma de asegurar su actualización y eficiencia. Las pruebas también deben asegurarse de que todos los miembros del equipo de recuperación y demás personal relevante tienen conocimiento de los planes.

Las pruebas deben indicar cómo y cuándo cada uno de sus componentes debe ser probada. Se recomienda probar los componentes individuales de los planes a menudo. Varias técnicas pueden ser utilizadas para asegurar la exactitud con la cual los planes operarán en la vida real.

Entre ellos, se destacan:

- Prueba de diferentes escenarios (discutiendo los acuerdo de recuperación, por ejemplo, usando interrupciones);
- Simulaciones (particularmente útiles para el entrenamiento del personal en sus puestos y funciones de gestión de la crisis);
- Pruebas de recuperación técnica (garantizando que los sistemas de información pueden ser efectivamente recuperados);
- Prueba de recuperación en un sitio alternativo (ejecutando los procesos de negocio de forma paralela con las operaciones de recuperación fuera de la sede principal);
- Pruebas de las instalaciones de los proveedores de servicios (asegurando que los servicios y productos suministrados por fuentes externas cumplen con los requisitos contratados);
- Ensayo completo (probando la organización, el personal involucrado, los equipos, las instalaciones de procesamiento y los procesos para confirmar que pueden enfrentar y superar las interrupciones del entorno de operación).

9.5.4 Mantenimiento y reevaluación

El plan de continuidad del negocio debe someterse a mantenimiento e intervalos regulares de tiempo, y actualizarse para asegurar su efectividad. Además de los cambios en los negocios, entre otros, se presentan a continuación, que pueden indicar la necesidad de mejoras en el plan, las pruebas realizadas deben estar completamente documentadas y sirven como fuente de datos para las actualizaciones.

Los cambios relevantes a ser considerados en el mantenimiento del plan incluyen la adquisición de nuevos equipos, nuevos sistemas (o actualización de los mismos), los cambios en las estrategias de negocio y los cambios en la legislación.

Se recomienda establecer responsabilidades para las revisiones regulares. La identificación de los cambios que han ocurrido en el negocio, pero aún no incluidas en el plan es una señal de que existe la necesidad de mantenimiento. El proceso de control de cambios debe garantizar que los planes actualizados serán distribuidos entre los sectores responsables (y para la sede remota, apropiadamente).

Ejemplo de recomendación para la continuidad del negocio: comprometiendo el entorno de las TI:

- "En caso de comprometimiento probado de seguridad del entorno de las TI por algún acontecimiento imprevisto, todas las

claves de acceso se deben cambiar. En estos casos, una versión segura del sistema operativo y del software de seguridad se debe descargar de nuevo, y los cambios recientes a los usuarios y los privilegios del sistema deben revisarse para detectar modificaciones no autorizadas a los datos."

El ejemplo presenta procedimientos recomendados que serán activados debido a la ocurrencia de desastres en el medio ambiente de las TI, cuyo objetivo es la continuidad del negocio.

Ejemplo de directriz para la concientización sobre la seguridad de la información y la continuidad del negocio:

» "La divulgación de reglas, riesgos, procedimientos y políticas de seguridad a los usuarios finales debe ser objeto de permanentes campañas internas, seminarios de sensibilización y cualquier otro medio o iniciativas para la consolidación de la educación para la seguridad de la información."

La directriz mostrada en el ejemplo comprende directamente la preocupación sobre la seguridad de la información y por consiguiente apoya en el sentido de garantizar la continuidad del negocio de la organización.

La Superintendencia Financiera de Colombia ha emitido circulares donde se normatiza la necesidad de que las entidades vigiladas por este ente de control obtengan un plan de continuidad de negocios, que cumplan con los siguientes elementos:

» Circular 041/2007- SARO: las entidades deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.
» Circular 038/2009 – Sistema de Control Interno: implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad para responder a las fallas e interrupciones específicas de un sistema o proceso y capacidad de retorno a la normalidad.

Ejercicio de nivelación - la gestión de incidentes de seguridad

» ¿Qué entiende usted por incidente de seguridad?
» ¿Qué se hace con los incidentes de seguridad en su institución?

En este tema serán presentados algunos de los principales aspectos de la seguridad de la información en las organizaciones: gestión de incidentes de seguridad, presentando así las preocupaciones con respecto a la notificación de incidentes y procedimientos necesarios para su gestión.

Estudie la sección 13. Gestión de incidentes de seguridad de la información y la mejora de la norma ISO/IEC 27002:2007.

La gestión de incidentes de seguridad de la información incluye una definición de responsabilidades y los procedimientos para el control efectivo de los eventos adversos (incidentes) después de la notificación. Por lo tanto, la gestión de incidentes involucra procedimientos para reportar los eventos adversos y la aplicación de medidas de seguridad adecuadas para su resolución. Vale la pena señalar que, además de la notificación, es importante un seguimiento efectivo de la organización como un medio para detectar los incidentes de seguridad.

9.6 Notificación de eventos adversos

Una serie de eventos adversos (incidentes o de seguridad) puede ocurrir en las organizaciones, como por ejemplo, pérdida de equipos y recursos, sobrecarga de sistemas; violaciones de los controles de acceso físico/lógico; malfuncionamiento de hardware/software, códigos maliciosos, negación de servicio (*Denial of Service,* DoS), uso inapropiado de los sistemas de información, entre otros.

El reporte de eventos adversos se debe hacer para aplicar las medidas correctivas adecuadas en el momento oportuno. Por lo tanto, es importante que todas las personas (empleados, contratistas, etc.) estén informadas acerca de los procedimientos formales para la notificación y por lo tanto se convierten en responsables de notificar cualquier evento adverso o vulnerabilidad que podría afectar la seguridad de la información de la organización.

Es de destacar que las notificaciones deberán ser enviadas al responsable (persona o equipo) directo de recibirlas en la organización. Por lo tanto, es importante identificar formalmente y por anticipado quién es la persona responsable. Por otra parte, se puede utilizar herramientas tales como formularios específicos para ayudar a las personas en la elaboración de la notificación y en el registro del evento adverso.

Ejercicio de refuerzo - notificación de los eventos adversos

» ¿Cuál es el propósito de la notificación de eventos adversos?

9.7 Procedimientos de gestión de incidentes de seguridad

Para la gestión de los incidentes de seguridad, debemos establecer los procedimientos adecuados a seguir después de su notificación. Estos procedimientos deben incluir las medidas efectivas que se adopten de manera ordenada y rápida.

Los procedimientos de gestión de incidentes de seguridad deben contemplar:

» Planes de contingencia;
» Identificación y análisis de la causa del incidente de seguridad. El análisis, en particular, proporcionar información sobre los tipos, cantidades y costos relacionados con los incidentes de seguridad con el fin de dar una idea del impacto de su ocurrencia a la organización (el negocio, principalmente) y por lo tanto dar indicios sobre necesidades en cuanto a la acción a tomar;
» Planificación y ejecución de medidas correctivas para evitar que se repita el incidente.

Una pregunta relevante se debe considerar: mantenimiento de procedimientos que determinan a quién contactar y cuándo ponerse en contacto en caso de incidentes relacionados con las autoridades, tales como estaciones de bomberos y agentes de vigilancia. El mantenimiento de esta información es importante tanto para la gestión de incidentes de seguridad como para la gestión de la continuidad del negocio.

El Departamento Nacional de Planeación de Colombia publicó, en julio de 2011, el documento CONPES 3701 que busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

Ejercicio de refuerzo - procedimientos de gestión de incidentes de seguridad

» ¿Qué procedimientos se deben considerar en la gestión de los incidentes de seguridad?

9.8 Planes de contingencia

Se presentarán los siguientes aspectos de la importancia de los planes de contingencia en las organizaciones y sus fases de planeamiento.

Implementar (planear, elaborar e implantar) un plan de contingencia involucra recursos financieros, acuerdos, cooperación de los empleados, y con frecuencia la asistencia de consultores técnicos externos y empresas especializadas en seguridad o seguros. Además, también se debe considerar los costos relacionados con entrenamiento, pruebas y mantenimiento del plan.

Un plan de contingencia debe incluir dos fases: la respuesta inmediata a los desastres (incluyendo incidentes de seguridad) y proceso de recuperación. En la primera fase, se deben considerar las decisiones gerenciales sobre las medidas que se aplicarán y, en la segunda fase, hay que definir los procedimientos necesarios para restaurar las funciones, los sistemas y recursos. El plan de contingencia puede incluir diferentes etapas (y complementarias) de recuperación, de modo que, a lo largo del tiempo, sea restablecido el funcionamiento normal de la organización.

A continuación se describen las fases que componen la planificación de contingencias y sus detalles.

Antes del planeamiento, es importante responder a las siguientes preguntas:

- ¿Cuáles son los objetivos?
- ¿Cuál es el presupuesto?
- ¿Cuáles son los plazos?
- ¿Cuáles son los recursos humanos disponibles?
- ¿Cuáles son los equipos y otros suplementos necesarios?
- ¿Cuáles son las responsabilidades del equipo responsables de la planificación?

Con todas las respuestas, usted puede comenzar el plan de contingencias, siguiendo las fases:

- Las actividades preliminares, que implican la conciencia de los líderes de la organización, la identificación de los recursos y la información crítica, análisis de costos y definición de plazos;
- Análisis de impacto, para identificar los impactos causados por la interrupción de los servicios proporcionados por el sistema informático de cada organización, teniendo en cuenta, por lo tanto, la importancia de cada uno de ellos para la continuidad del negocio;
- El análisis de alternativas de recuperación, que procura verificar la relación costo/beneficio de las diversas opciones para la recuperación de desastres. Es importante que, justo después de esta etapa, sea elaborado y se entregue a los líderes de la organización un documento informando el análisis y recomendaciones para la continuidad del negocio;
- Desarrollo del plan de contingencia después de analizar el informe presentado al final de la fase anterior, tiene como objetivo elaborar el contenido del plan;
- Entrenamiento, con el objetivo de concientizar a las personas acerca de sus responsabilidades con respecto al plan;
- Prueba del plan de contingencias, buscando identificar las mejoras a través de adaptaciones o correcciones;
- Evaluación de los resultados y actualización del plan, en el cual los resultados de las pruebas son evaluados e iniciando el proceso de modificar el plan conforme a las mejoras propuestas.

Las actividades preliminares

- Las iniciativas para la concientización de los dirigentes.
- Estudio preliminar de los recursos, los sistemas y las funciones críticas del negocio
- Las actividades preliminares de planificación de contingencias cubren básicamente todas las iniciativas de sensibilización de líderes sobre las necesidades y un estudio preliminar sobre los ítems críticos para la organización.

No se puede implementar un plan de contingencia sin una sensibilización de los dirigentes de la organización, y mucho menos sin su apoyo total.

En el estudio preliminar de los servicios críticos, son recopilados recursos, sistemas y funciones críticas de los negocio de la organización, así como el costo, los plazos y los recursos humanos necesarios en la realización del análisis de impacto (la próxima fase de planificación). Note aquí la importancia de presentar este estudio a los líderes de la organización, con la intención de obtener su aprobación.

Ejercicio de refuerzo - los planes de contingencia

- ¿ Cuáles son las fases de un plan de contingencias y qué debe ser considerado en cada fase?
- ¿ Cuáles son las actividades preliminares de la planificación de contingencia?

9.9 Análisis de impacto

En esta fase se identifican y se clasifican, de acuerdo con su importancia para el negocio de la organización, las funciones, los sistemas y recursos, teniendo en cuenta, por tanto, las posibles amenazas a que están expuestos. Este análisis es un elemento importante para que los dirigentes puedan tomar decisiones con respecto a las inversiones que serán aplicadas en medidas de seguridad para la continuidad de su negocio.

En el proceso de análisis de impacto, es importante llevar a cabo entrevistas con los diferentes gerentes de los sectores específicos y críticos para los negocios de la organización, equipos de soporte y usuarios de sistemas.

El análisis de impacto se puede dividir en tres sub-fases: identificación de recursos, funciones y sistemas críticos, definición del tiempo para la recuperación y elaboración de informes.

Figura 29.
Secuencia hasta el impacto

Ejercicio de refuerzo - análisis de impacto

» Especifique las sub-fases de un análisis de impacto.

9.10 Identificación de recursos, funciones y sistemas críticos

En esta sub-fase, se debe considerar tanto la identificación de los recursos, funciones y sistemas críticos, como su clasificación. La siguiente es una propuesta de clasificación que se puede utilizar en organizaciones reales:

» Altamente importante (esenciales);
» Importancia media;
» Baja importancia.

Tenga en cuenta que la identificación y clasificación generan datos escenciales para la toma de decisiones en relación con el alcance del plan de contingencia, garantizando el funcionamiento de la organización en un nivel de servicio aceptable.

9.11 Definición del tiempo para la recuperación y elaboración del informe

En la sub-fase de definición del tiempo para la recuperación se determina el rango de tiempo aceptable de indisponibilidad de cada función, recurso y sistema de acuerdo con la criticidad y el impacto relativo. Como resultado se tiene un intervalo de tiempo aceptable para la recuperación del recurso, sistema o función.

En el informe, se debe destacar:

- Los recursos, los sistemas y las funciones identificadas y clasificadas por orden de importancia para la organización;
- Una descripción de las amenazas potenciales para cada recurso, sistema y función;
- El rango de tiempo tolerable para la recuperación de cada recurso, sistema y función;
- La recopilación de la información sobre recursos humanos, instalaciones, equipos y servicios requeridos para la restauración y la recuperación de cada recurso, sistema y función.

Al final de las tres sub-fases el informe permitirá a los líderes de la organización la toma de decisiones con respecto a la implementación del plan de contingencia.

9.12 Análisis de alternativas de recuperación

En esta fase, las alternativas, tales como la prevención y la detección de accidentes, control de *backups*, estrategias confiables para almacenar y recuperar datos, seguros, redundancia de sistemas y recursos, entre otras alternativas de recuperación en caso de desastres son analizadas y seleccionadas para ser implantadas en casos específicos de necesidad de contingencia, teniendo en cuenta los resultados obtenidos en las etapas anteriores de planificación.

En términos de prevención y detección de accidentes, se recomienda tener en cuenta los equipos de detección y extinción de incendios; el mantenimiento preventivo de los equipos, la protección de los documentos no magnéticos (impresos, por ejemplo); la seguridad adecuada de los recursos humanos, etc.

La política de *backup* es uno de los elementos más importantes de un plan de contingencia, después de todo, un sistema que ha experimentado problemas se puede comparar con su *backup* (si se mantiene actualizado y completo), lo que permite su restauración. Por lo tanto, es la política de copia de seguridad la que determina todos los procedimientos necesarios para la protección de la información de la organización de acuerdo a su importancia para el negocio. Recuerde que la infraestructura y los procedimientos de *backup* deben someterse a pruebas regulares, para que la recuperación en caso de problemas de seguridad esté realmente asegurada.

En términos de almacenamiento de datos, se debe considerar la seguridad adecuada aplicada a los medios y el lugar de almacenamiento utilizado, inclusive teniendo en cuenta el almacenamiento remoto de las copias de seguridad. Para la recuperación de los datos almacenados, se recomienda comprobar regularmente los procedimientos de restauración utilizados. Recuerde que si la recuperación de los datos fracasa, de nada sirve mantener las copias de seguridad.

También se debe considerar la posibilidad de contratar un seguro para cubrir posibles pérdidas causadas por incidentes de seguridad.

Ejercicio de refuerzo - análisis de alternativas de recuperación

» ¿Por qué una política de *backup* es importante en un plan de contingencia?

9.13 Informes de alternativas de recuperación

Después del análisis de las alternativas se debe elaborar un informe detallado sobre las opciones de recuperación, estimaciones de costos, ventajas y desventajas de cada alternativa.

Tenga en cuenta también los recursos humanos, financieros y de infraestructura necesarios para la próxima fase. Este informe también prestará apoyo a la dirección de la organización en la toma de decisiones estratégicas en relación con el plan de contingencia.

9.14 El desarrollo del plan de contingencia

Durante el desarrollo de un plan de contingencia se debe prestar atención a las siguientes pautas:

» Designar un equipo para implementar el plan de contingencia, inclusive dividiéndolo por área de actuación. Por ejemplo, el equipo gerencial, que se ocupará de la coordinación de las actividades relacionadas, y el equipo de respuesta inmediata a incidentes que activan las medidas apropiadas a los incidentes de seguridad ocurridos;
» Determinar la forma de responder a los desastres en el momento oportuno, abarcando la identificación y comprensión del problema, contención de daños; identificación de daños causados; restauración de los sistemas y eliminación de las causas de los desastres;
» Identificar los aplicativos críticos, a los que se deben aplicar las medidas de emergencia en situaciones de desastre;
» Mantener un registro (o inventario) de archivos, datos, programas, sistema operativo y utilitarios relacionados con los aplicativos críticos, asegurando que todos están incluidos en los procedimientos de respaldo y recuperación;
» Recopilar las necesidades de condiciones especiales requeridas por las redes de comunicación;

» Tener en cuenta la retirada del personal y la garantía de la seguridad de los documentos en papel y medios magnéticos.

9.15 Entrenamientos y pruebas

Se deben considerar en esta fase iniciativas para crear conciencia en los empleados y terceros en relación con el plan de contingencia de la organización. Por lo tanto, los entrenamientos deben ser regulares, involucrando la teoría, la práctica y las simulaciones.

Una de las garantías que la organización puede considerar, en términos de plan de contingencias, es el resultado de las pruebas que se le aplican. En términos prácticos, las pruebas se pueden clasificar en las siguientes categorías:

» Integral, involucrando situaciones cercanas a la realidad de la organización, por ejemplo, contemplando la verificación de procedimientos de traslado de personas y procesamiento a los sitios alternos;
» Parcial, limitada a partes del plan de contingencia o a determinadas actividades o aplicativos;
» Simulada, considerando representaciones de la situación de desastre, por ejemplo, la evacuación del edificio de la organización en un simulacro de incendio.

Durante las pruebas, se debe cronometrar todos los eventos relacionados y registrar cualquier problema que ocurra, si es posible indicando una clasificación de acuerdo a su gravedad.

Ejercicio de refuerzo - formación y pruebas

» ¿Cómo se pueden clasificar las pruebas?

9.16 Evaluación y actualización del plan

Debido a los cambios en los objetivos de negocio, cambios administrativos y en el ambiente computacional, por ejemplo, también se debe actualizar el plan de contingencia, de manera que este refleje los cambios, minimizando los impactos causados por fallas de seguridad.

Los ejemplos de las recomendaciones para la prevención de incidentes de seguridad de la información:

- "no está permitido, a menos que se cuente con la debida autorización, interferir, sobrecargar o deshabilitar un servicio, incluyendo unirse o cooperar con ataques de negación de servicios internos o externos."
- "Se prohíbe a los usuarios la ejecución de pruebas o tentativas que comprometa los controles internos. Esta práctica sólo se permite a personas con competencia y función técnica en la organización, durante actividades de monitoreo y análisis de riesgos, con la autorización legítima para hacerlo."

Estos ejemplos presentan algunas recomendaciones que podrían ser parte de la política de seguridad o de las directrices para la seguridad de la información, enfocados a la ocurrencia de incidentes de seguridad. Todas las recomendaciones se consideran genéricas y aplicables a organizaciones reales.

9.17 Buenas prácticas

En la búsqueda de una adecuada gestión de incidencias y un plan de contingencia efectivo para una organización, se recomiendan algunas prácticas:

- Documentar todos los incidentes de seguridad y las acciones tomadas, para permitir una investigación posterior de las causas;
- Identificar recursos, funciones y sistemas críticos y sus prioridades para el negocio;
- Analizar el impacto causado por las amenazas de seguridad de la organización;
- Evaluar las alternativas de recuperación, buscando identificar las más adecuadas para el contexto;
- Elaborar el plan de contingencias de acuerdo con los recursos disponibles (financieros, recursos humanos y de infraestructura);
- Entrenar a las personas, concientizándolas sobre sus responsabilidades acerca del plan de contingencias;
- Llevar a cabo pruebas periódicas del plan de contingencias y los procedimientos de recuperación establecidos en la organización.

Capítulo

10

Conformidad

Objetivos

Verificar la conformidad con las políticas y normas de seguridad de la información y evaluar el cumplimiento de la legislación.

Conceptos

Legislación y derechos informáticos en Colombia, el cumplimiento de los requerimientos legales y de auditoría.

10.1 Legislación y derecho informático en Colombia

En cuanto a la legislación y derecho informático en Colombia, se presentarán los siguientes subtemas:

- Importancia de la legislación, mostrando los elementos relevantes, en términos de la legislación, para la seguridad de la información;
- Derecho informático, presentando la definición y cuestiones relacionadas;
- Legislación y derecho informático en Colombia, dando una visión general sobre las leyes vigentes, con respecto a tecnología y seguridad de la información
- Derecho informático y las necesidades actuales, identificando las necesidades actuales en cuanto a la ausencia de una legislación específica en materia del derecho informático en Colombia;
- Caso de estudio, con el objetivo de presentar una actividad práctica correspondiente, con el fin de proporcionar a los participantes una reflexión sobre las posibles medidas preventivas para el caso estudiado.

Ejercicio de nivelación - conformidad

- ¿Qué entiende usted por conformidad?
- ¿Cómo está implementada la conformidad en su institución?

10.2 Importancia de la legislación

Los aspectos legales específicos deben ser considerados (la legislación varía de un país a otro).

Existe una creciente preocupación por la legislación y las normas relacionadas con la seguridad de la información, dada su importancia para la sociedad actual. De este modo, varios proyectos legislativos, estándares y normas se han definido o están en curso o en desarrollo.

La Ley, en particular, garantiza la protección de los derechos aplicables a la seguridad de la información y prevé sanciones legales en situaciones de fraude. Sobre la base de los estándares y normas, las organizaciones pueden establecer sus políticas de seguridad y el proceso de auditoría adaptados a su ramo de negocio. Vale la pena aclarar que, en la mayoría de los casos, los estándares tienen alcance internacional, mientras que las normas y leyes son a nivel nacional. Por lo tanto, hay variaciones en cuanto a los estándares, normas y leyes que se aplican en los distintos países

Las organizaciones deben garantizar la protección contra la violación de cualquier Ley penal o civil, estatutos, reglamentaciones, obligaciones contractuales y requisitos de seguridad de la información, con el objetivo de garantizar el cumplimiento legal y la salud institucional. En este contexto, se recomiendan los servicios de consultoría prestados por organizaciones o profesionales especializados en el área jurídica (derecho informático) y de seguridad de la información

En la búsqueda del cumplimiento legal, es saludable que la organización busque y se mantenga actualizada sobre la legislación vigente y las normas y estándares de seguridad aplicables. En Colombia, el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, establece las normas que deben seguir los productos y servicios, incluidos los relacionados con la seguridad de la información. A nivel internacional, se destacan en el área, la *International Organization for Standardization*, ISO y la *International Electrotechnical Commission*, IEC.

Entre las normas directamente relacionadas con la gestión de la seguridad de la información, se destacan las normas NTC ISO/IEC 27001:2005 y NTC ISO/IEC 27002:2007.

10.3 Derecho informático

El derecho informático comprende un conjunto de principios fundamentales e instrumentos jurídicos que responden a requisitos de la era digital que implican cuestiones multidisciplinarias relevantes: civil, laboral, constitucional, del consumidor, penal, derechos de autor y contractual.

Los siguientes son ejemplos de cuestionamientos relativos a las materias tratadas en el ámbito del derecho informático:

- En materia civil. Por ejemplo, el montaje de una página web falsa en internet, afectando a una organización determinada, ¿puede dar lugar a una indemnización por daños morales y materiales?
- En materia laboral. Por ejemplo, ¿el despido de un empleado por el mal uso del correo electrónico puede ser caracterizado como una causa justa?
- En materia constitucional. Por ejemplo, ¿el seguimiento de los correos electrónicos de los empleados viola el derecho a la privacidad?
- En materia del consumidor. Por ejemplo, ¿compartir los datos recopilados en internet infringe el Estatuto del Consumidor (Ley 1480 de octubre de 2011)?
- En materia Penal. Por ejemplo, si un empleado instala software pirata en su computador de trabajo, ¿la organización responde judicialmente?
- En materia de derechos de autor. Por ejemplo, ¿tiene la organización el derecho al código fuente del software contrata con terceros?
- En materia contractual. Por ejemplo, ¿los e-mails intercambiados entre las partes pueden ser utilizados como prueba de una relación contractual?

Ejemplo de recomendación para el uso de los recursos de las TI definida en la política de la seguridad:

- "Sólo las actividades lícitas, éticas y administrativamente permitidas deben ser realizadas por el usuario dentro de la infraestructura de las TI, dejando a los infractores sujetos a la Ley penal, civil y administrativa, en el grado de conducta, dolosa o culposa, que practiquen."

La recomendación propuesta en el ejemplo es aplicable a las organizaciones, una vez que sea debidamente documentada en la política de seguridad y que se haga efectiva en la organización, es decir, debidamente implementada, comunicada y exigida.

Ejercicio de refuerzo - derecho informático

» ¿Qué es el derecho informático y cómo se aplica en su organización?

10.4 Legislación y derecho informático en Colombia

Algunas Leyes relacionadas con derecho informático en Colombia.

» Derechos de autor, Ley 23 de 1982
» Constitución Política de Colombia de 1991
» Propiedad Industrial, Ley 178 de 1994:
» Comercio electrónico, la ley 527 de 1999
» Nuevo estatuto penal, Ley 906 de 2004
» Habeas Data, Ley 1266 de 2008
» Delito Electrónico, Ley 1273 del 2009
» Tecnologías de la Información y las Comunicaciones, Ley 1341 de 2009
» Nuevo Estatuto del Consumidor, La Ley 1480 de 2011
» Ley de transparencia y acceso a la información pública nacional, Ley 1712 de 2014

Se recomienda la revisión del anexo 1 adjunto a este documento.

La tecnología de la información avanza a pasos largos y consolida la era digital y poco a poco las leyes que conforman el derecho informático en Colombia siguen esta evolución.

Es importante destacar, además, que existe responsabilidad civil y penal para aquellos que trabajan con la seguridad de la información y la tecnología de la información en Colombia. Por lo tanto, las organizaciones públicas y privadas, los funcionarios públicos y los empleados deben conocer sus responsabilidades y obligaciones legales.

10.5 Legislación aplicable a la seguridad de la información

» **Derechos de Autor**
- Decisión 351 de la C.A.N.
- Ley 23 de 1982
- Decreto 1360 de 1989
- Ley 44 de 1993
- Decreto 460 de 1995
- Decreto 162 de 1996
- Ley 545 de 1999
- Ley 565 de 2000
- Ley 603 de 2000
- Ley 719 de 2001

» **Propiedad Industrial**
- Decisión 486 de la C.A.N.
- Decreto 2591 de 2000
- Ley 463 de 1998
- Ley 170 de 1994
- Ley 178 de 1994

» **Propiedad intelectual**
- Decisión 345 de la C.A.N.
- Decisión 391 de la C.A.N.
- Decisión 523 de la C.A.N.

» **Comercio electrónico y firmas digitales**
- Ley 527 de 1999
- Decreto 1747 de 2000
- Resolución 26930 de 2000

» **Ley 1273 de 2009, añade dos nuevos capítulos al Código Penal Colombiano:**
- Capítulo primero: de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
- Capítulo segundo: de los atentados informáticos y otras infracciones.

» Ley 603 de 2000: esta Ley se refiere a la protección de los derechos de autor en Colombia.

» Ley Estatutaria 1266 del 31 de diciembre de 2008: por la cual se dictan las disposiciones generales del Habeas Data y se re-

gula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

» Ley 1273 del 5 de enero de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

» Ley 1341 del 30 de julio de 2009: por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

» Ley estatutaria 1581 de 2012: de protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

» Decreto 1377 de 2013: protección de datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Enlaces de interés:

» Presidencia de la República de Colombia
http://wsp.presidencia.gov.co/Normativa/Leyes/Paginas/2014.aspx
» Ministerio de Tecnologías de la Información y las Comunicaciones
http://www.mintic.gov.co/
» Grupo de Respuesta a Emergencias Cibernéticas de Colombia
http://www.colcert.gov.co/
» A través de la Política Nacional de Ciberseguridad y Ciberdefensa Nacional, tiene como objetivo la coordinación de los temas de Ciberseguridad y Ciberdefensa y la protección de la Infraestructura Crítica Nacional.
» Centro Cibernético Policial
http://www.ccp.gov.co/

El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

Ejercicio de refuerzo - legislación aplicable a la seguridad de la información

» ¿Cuál es el propósito de la Ley 1341 del 30 de julio de 2009?

10.6 Ejemplos de infracciones informáticas

La siguiente tabla muestra ejemplos de infracciones informáticas que se producen en el medio corporativo con la caracterización del artículo de la Ley, el delito y la pena a pagar:

Tabla 12. Delitos informáticos en el entorno empresarial

Artículos de la Ley 1273 del 2009	Se comete delito cuando	Pena
269 A: Acceso abusivo a un sistema informático	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 B: Obstaculización ilegítima de sistema informático o red de telecomunicación	Bloquean en forma ilegal un sistema o impiden su ingreso, igualmente, el acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 C: Interceptación ilícita de datos informáticos	Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses

Continuación tabla 12. Delitos informáticos en el entorno empresarial

Artículos de la Ley 1273 del 2009	Se comete delito cuando	Pena
269 D: Daños informáticos	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de las TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 E: Uso de software malicioso	Cuando se producen, adquieren, distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos de las TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 F: Violación de datos personales	Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 G: Suplantación de sitios web para capturar datos personales	Crean una página similar a la de una entidad y envía correos (spam o engaños), como ofertas de empleo y personas inocentemente, suministran información personal y claves bancarias, y el delincuente informático ordena transferencias de dinero a terceros.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

Fuente. Adaptación propia tomada de Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.

10.7 Derecho informático y necesidades actuales

En cuanto a las necesidades actuales en materia de legislación y del derecho informático, hay una serie cuestiones sin definir, como las que se ejemplifican a continuación:

- Privacidad versus monitoreo, por ejemplo, cuando los empleados utilizan la dirección de correo electrónico corporativo para recibir contenido privado;
- Seguridad de la información versus usuario, en particular, para establecer con claridad los derechos y sanciones legales aplicables en caso de problemas;

- La responsabilidad por actividades realizadas en equipos de la organización son relevantes porque los equipos son activos y se deben utilizar con el fin de no ocasionar procesos judiciales;
- Límites de responsabilidad en ambientes externos, deben ser considerados cuando se trata de soluciones como el acceso remoto a la red o la organización o soluciones de oficina en casa;
- En cuanto a la necesidad de la custodia de evidencias, documentos digitales, tales como e-mail, no tienen una legislación específica que determine su uso como evidencia.

Si bien la legislación referente al derecho informático no está plenamente establecida, reglas claras para la conducta de los empleados, directores, contratistas y otras personas involucradas deben ser desarrolladas por las organizaciones. Tal conducta debe ser monitoreada y controlada y los usuarios debidamente orientados adecuada acerca de sus límites y responsabilidades por las acciones tomadas en la organización. Siempre es importante recordar que divulgar y orientar son los dos factores principales para limitar riesgos.

10.8 Ley de acceso a la información

Ley de transparencia y acceso a la información pública nacional, Ley 1712 del 6 de marzo de 2014.

- **Artículo 1. Objetivo.** Tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
- **Artículo 2. Principio de máxima publicidad para titular universal.** Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente Ley.
- **Artículo 3. Otros principios de la transparencia y acceso a la información pública.** En la interpretación del derecho de acceso a la información se deberá adoptar un criterio de razonabilidad y proporcionalidad, así como aplicar los siguientes principios:
  - **Principio de transparencia.** Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta Ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto

establezca la Ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta Ley.

- **Principio de buena fe.** En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.
- **Principio de facilitación.** En virtud de este principio los sujetos obligados deberán facilitar el ejercicio del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.
- **Principio de no discriminación.** De acuerdo al cual los sujetos obligados deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivación para la solicitud.
- **Principio de gratuidad.** Según este principio el acceso a la información pública es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.
- **Principio de celeridad.** Con este principio se busca la agilidad en el trámite y la gestión administrativa. Comporta la indispensable agilidad en el cumplimiento de las tareas a cargo de entidades y servidores públicos.
- **Principio de eficacia**. El principio impone el logro de resultados mínimos en relación con las responsabilidades confiadas a los organismos estatales, con miras a la efectividad de los derechos colectivos e individuales.
- **Principio de la calidad de la información.** Toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad.
- **Principio de la divulgación proactiva de la información.** El derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de promover y generar una cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros.

- **Principio de responsabilidad en el uso de la información.** En virtud de este, cualquier persona que haga uso de la información que proporcionen los sujetos obligados, lo hará atendiendo a la misma.

El Presidente Juan Manuel Santos sancionó el 6 de marzo de 2014 la Ley 1712 de 2014 que les permite a los colombianos exigir su derecho a la información como un derecho fundamental.

El diseño, promoción e implementación de la política pública de acceso a la información pública está a cargo de la Secretaría de Transparencia de la Presidencia de la República, el Ministerio de Tecnología de la Información y Comunicaciones, el Departamento Administrativo de la Función Pública, DAFP, el Departamento Nacional de Planeación, DNP, el Archivo General de la Nación y el Departamento Administrativo Nacional de Estadística, DANE. Se obliga a las entidades a garantizar que las personas en condición de discapacidad y los diferentes grupos étnicos y culturales accedan a información de su interés.

El derecho de acceso a la información pública implica que las entidades no solamente deben responder a las solicitudes expresas de información de los ciudadanos, sino también divulgarla proactivamente y responder a los requerimientos de forma rutinaria, proactiva, actualizada, accesible y comprensible.

La Ley 1712 de 2014 establece excepciones al acceso a la información en los casos de información clasificada siempre que el acceso pudiere causar daño a los derechos de las personas a la intimidad, la vida, la salud, la seguridad. También exceptúa la información relacionada con secretos comerciales, industriales y profesionales.

De igual manera, toda información pública reservada es exceptuada por daño a los intereses públicos siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional (la defensa y seguridad nacional, la seguridad pública, las relaciones internacionales, el debido proceso y la igualdad de las partes en los procesos judiciales, la administración efectiva de la justicia, los derechos de la infancia y la adolescencia, la estabilidad macroeconómica y financiera del país, la salud pública, entre otras).

En este punto, se destaca la importancia del área de las TI de la organización así como los procedimientos relativos a seguridad de la información para ser preservada la confidencialidad y la privacidad cuando fuere el caso. Otro punto importante es que con el fin de procesar adecuadamente la información, la organización necesita para poner en

práctica una política de información clasificada (véase el punto 7.2 de la norma ISO/IEC 27002:2007).

10.9 Verificación de conformidad con los requisitos legales

En cuanto a la verificación del cumplimiento de los requisitos legales, se presentarán los siguientes subtemas:

La legislación vigente, mostrando los aspectos importantes a considerar en términos de los documentos legales de la propia organización y de la legislación vigente en Colombia.

Los temas propiedad intelectual, protección de los registros de la organización, protección de datos y privacidad de la información personal, la prevención del uso indebido de recursos de procesamiento de información y los controles criptográficos son presentados con el fin de indicar algunas de las preocupaciones sobre seguridad de la información y las leyes vigentes en las organizaciones. En particular, estos temas se documentan como recomendaciones en las normas NTC ISO/IEC 27001:2005 y NTC ISO/IEC 27002:2007.

10.10 La legislación vigente

Es importante en las organizaciones considerar la legislación en términos de estatutos, reglamentos y contratos vigentes, además de considerar la legislación específica y actual en el país. De esta forma, todos los requisitos involucrados en estos ítems deberán ser definidos, mantenidos y documentados por la organización.

Al mismo tiempo, también es importante definir y documentar todos los controles y responsabilidades necesarias para garantizar los requisitos estatutarios, reglamentarios y contractuales.

10.11 Propiedad intelectual

Se recomienda implementar procedimientos para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales.

Se recomienda para cualquier material o software propietario protegido por la Ley de propiedad intelectual, poner en práctica procedimientos adecuados para asegurar el cumplimiento de la organización con respecto a los requisitos legales, reglamentarios y contractuales.

Por ejemplo, estos requisitos pueden determinar restricciones a la copia de determinado material con derechos de autor, o aunque solamente sea utilizado material desarrollado por la propia organización.

Es importante aplicar cuidados contra la violación de la propiedad intelectual, sobre todo porque esta situación puede dar lugar a demandas civiles e incluso penales.

10.12 El cuidado de la propiedad intelectual

Como hemos visto, las organizaciones deben estar preocupadas por la propiedad intelectual y por lo tanto poner en práctica los procedimientos adecuados, que culminan con la protección de las organizaciones frente a aspectos legales, estatutarios y contractuales. Por ello, la norma NTC-ISO/IEC 27002:2007 recomienda algunos cuidados relevantes:

- La divulgación de una política de cumplimiento de los derechos de propiedad intelectual que, a su vez, define claramente el uso legal de cualquier material, software o información protegida contra las infracciones a la propiedad intelectual;
- En los procesos de adquisición de software, esto deben ser obtenidos únicamente de fuentes reconocidas y acreditadas;
- Mantener a todos en la organización, independientemente del cargo, conscientes de las políticas de protección de la propiedad intelectual y de las medidas disciplinarias que se aplicarán en los casos de infracción;
- Indicar cada activo de la organización que tenga requisitos directamente relacionados con la protección de los derechos de la propiedad intelectual, incluso manteniendo su registro adecuado;
- Mantener todas las evidencias sobre licencias, manuales y similares en la organización.

Monitorear las licencias, para asegurar que no se exceda el uso del número máximo de licencias adquiridas.

- Efectuar el control de software garantizando la instalación únicamente de aquellos que tienen licencia y están debidamente autorizados;
- Implementar una política para el mantenimiento adecuado de las condiciones de las licencias;
- Definir una política para regular la transferencia de software a otras organizaciones;
- Asegurarse de que las herramientas de auditoría utilizadas son adecuadas;
- Satisfacer todos los términos y condiciones de los materiales, el software y la información obtenida de las redes públicas;
- Proteger los registros de negocios, tales como películas, audios y otros, contra las duplicaciones, conversiones o extracciones no permitidas por las leyes de derechos de autor;
- Proteger partes o la totalidad de libros, artículos, informes, etc., contra copias no autorizadas e infracción de la Ley de derechos de autor vigente.

Los productos de software propietario son proporcionados mediante un contrato de licenciamiento que define los términos y las condiciones de la licencia, como por ejemplo, limitando la copia del software sólo para crear una copia de seguridad.

Se aplican los derechos de propiedad intelectual sobre el software, documentos, diseños, marcas registradas, patentes y licencias de código fuente.

Ejercicio de refuerzo - cuidados de la propiedad intelectual

- Nombre tres cuidados de la propiedad intelectual adoptados en su institución.

10.13 Protección de los registros de la organización

- En las organizaciones, se recomienda proteger los registros considerados como esenciales para el negocio contra pérdida, destrucción y falsificación, para garantizar el cumplimiento de sus requisitos legales, reglamentarios y contractuales.
- Algunos registros pueden precisar ser conservados de forma segura para satisfacer los requisitos legales, contractuales o reglamentarios, o incluso responder a los requerimientos del negocio. Por ejemplo, aquellos registros que evidencian el cumplimiento de una organización ante los requisitos legales, reglamentarios y contractuales, lo que garantiza la defensa de la organización contra acciones legales, civiles o penales.
- Además, los registros también se pueden clasificar con el fin de aplicar las definiciones específicas, tales como el período de retención y el tipo de medios de almacenamiento. Por ejemplo, los registros de auditoría, los registros contables y los registros de las transacciones deberán tener un tiempo de retención de 6 meses, de 1 año y de 3 meses, almacenados en medios magnéticos, papel y medio magnético, respectivamente.
- Las claves de criptografía utilizadas para asegurar la confidencialidad y la autenticidad de los registros también deben ser almacenados durante el tiempo de retención respectiva.
- Además, se considera que todos los medios de almacenamiento estarán protegidos contra el deterioro si se utilizan de acuerdo con las recomendaciones del proveedor.
- El tiempo de retención aplicado a registros de la organización (Tabla de Retención Documental, TRD) está definido en las Leyes y reglamentos nacionales, tales como el Decreto 1382 de 1995 y la Ley 594 del 2000 y otros que regulan el Archivo General de la Nación.

Mayor información con respecto la Gestión de Archivos puede encontrarse en la Norma ISO 15489-1 Gestión de documentos de archivo

10.14 Cuidados para la protección de los registros de la organización

Para asegurar la protección de los registros de una organización, la norma NTC-ISO/IEC 27002:2007 recomienda los siguientes procedimientos:

- El establecimiento de directrices para la retención, el almacenamiento, el procesamiento y la disponibilidad de los registros y la información
- Definir un cronograma para la retención, para indicar los registros esenciales y su periodo respectivo en el que se aplicará;
- Mantener un inventario que comprende fuentes de información que se considere fundamentales para la organización;
- Implementar controles adecuados para la protección de registros e información.

Consulte las normas y recomendaciones del Archivo General de la Nación (AGN): http://www.archivogeneral.gov.co.

10.15 Protección de los datos y privacidad de la información personal

En las organizaciones se recomienda garantizar la protección de datos y privacidad de la información personal, de acuerdo con las leyes, reglamentaciones y contratos vigentes.

Para ello, las organizaciones pueden crear un equipo que va a definir, implementar, divulgar y gestionar una política de protección y privacidad, buscando al mismo tiempo la conformidad con las leyes, reglamentaciones y contratos vigentes. Es de destacar que todas las personas de la organización deben ser orientadas para saber exactamente cuáles son sus responsabilidades en virtud de la política.

Algunos países tienen leyes que establecen el control en la recolección, procesamiento y transmisión de datos e información personal, imponiendo responsabilidades legales a los directamente involucrados en estas etapas.

El 17 de octubre de 2012 el Gobierno Nacional colombiano expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones

generales para la protección de datos personales. En ella se regula el derecho fundamental de *hábeas data* y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C–748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención.

La Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada.

El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

10.16 Prevención del mal uso de los recursos de procesamiento de información

En las organizaciones, los recursos de procesamiento de la información apoyan el negocio, por lo tanto, se recomienda proteger los recursos de procesamiento de la información contra el uso no autorizado o con objetivos no relacionados con el negocio. Para ello, se puede emplear, por ejemplo, un monitoreo adecuado, herramientas de apoyo (IDS, *Intrusion Detection Systems*), acciones disciplinarias o legales. En cuanto al monitoreo y al uso de herramientas, debe prestar atención a la legislación vigente. A menudo, la organización debe divulgar a todos los usuarios que los recursos de procesamiento de la información están siendo monitoreados.

En cuanto a los usuarios, una buena práctica es concientizarlos sobre sus derechos y deberes ante los recursos de procesamiento disponibles en la organización y la legislación vigente. A modo de ejemplo, se puede exigir a los usuarios el firmar una declaración de conocimiento de sus responsabilidades en el contexto. Por lo tanto, tales declaraciones deben mantenerse a salvo en la organización.

10.17 Controles criptográficos

En las organizaciones, el uso de la criptografía debe llevarse a cabo de conformidad con las Leyes, reglamentos, contratos y acuerdos. Por lo tanto, la norma NTC-ISO/IEC 27002:2007 recomienda las siguientes acciones, de conformidad con la legislación nacional vigente:

- Restringir el uso de la criptografía;
- Restringir la importación y / o exportación de hardware y software destinado a la ejecución de funciones criptográficas;
- Restringir la importación y / o exportación de hardware y software diseñado con funciones embebidas (integradas) de criptografía;
- Definir métodos de acceso a la información encriptada por hardware o software que serán utilizada por autoridades de otros países.

Ejemplo de recomendación para el uso de los recursos de las TI definida en la política de seguridad:

- "Los sistemas de las TI deben utilizarse sin violar los derechos de propiedad intelectual de cualquier persona u organización, tales como marcas y patentes, nombres comerciales, secreto empresarial, dominio en internet, diseño industrial o cualquier otro material que no tenga autorización expresa del autor o propietario de los derechos a la obra artística, científica o literaria."

La recomendación propuesta en el ejemplo es aplicable a las organizaciones destinadas a la protección de la propiedad intelectual una vez que esté bien documentada en la política de seguridad y que se haga efectiva en la organización, es decir, debidamente implementada, divulgada y exigida.

10.18 Verificación del cumplimiento de las políticas y normas de seguridad de la información

En cuanto a la verificación del cumplimiento de las políticas y las normas de seguridad de la seguridad de la información, se presentarán los siguientes sub-temas: "Normas de seguridad en Colombia", mostrando las principales normas vigentes para el contexto. En el tema "Evolución

de las normas", se indica una prospección en cuanto a su mantenimiento. Los temas "Cumplimiento de las políticas y normas" " Trabajando las no conformidades" y "Conformidad Técnica" presentan individualmente las preocupaciones y prácticas a tener en cuenta en relación con las políticas y normas en las organizaciones.

10.18.1 Las normas de seguridad en Colombia

En 2005, ICONTEC dio a conocer la norma NTC-ISO/IEC 17799, una versión colombiana de BS ISO/IEC 17799, y desde entonces, en Colombia, esta norma se ha convertido en una de las principales referencias para la gestión de seguridad de la información. En su contenido, la norma se ocupa de los siguientes temas: la política de seguridad de la información, organización de la seguridad información, gestión de activos, la seguridad de los recursos humanos, la seguridad física y el medio ambiente, la gestión de las comunicaciones y operaciones, control de acceso, la adquisición, desarrollo y mantenimiento de sistemas de información, gestión de incidentes de seguridad de la información, gestión de la continuidad del negocio y el cumplimiento.

La siguiente es la historia del desarrollo de los estándares y normas internacionales en Colombia:

- En 1995, se lanzó la primera versión de BS 7799-1 (BS 7799-1:1995 - Tecnología de la información - Código de buenas prácticas para la gestión de seguridad de la información).
- En 1998, se lanzó la primera versión de BS 7799-2 (BS 7799-2:1998 - Gestión del sistema de seguridad de la información - Especificaciones y guías para su uso).
- En 1999, se lanzó la revisión de la norma BS 7799-1:1995.
- En 2000, se lanzó la primera versión de la norma BS ISO / IEC 17799
- (BS ISO / IEC 17799:2000 - Tecnología de la información - Código de buenas prácticas para la gestión de seguridad de la información).
- En 2005, se aprobó por ICONTEC la 17799 versión colombiana de BS ISO / IEC 17799 (ISO/IEC 17799:2004 - Tecnología de la información - Código de buenas prácticas para la gestión de seguridad de la información).
- En marzo de 2006 fue ratificada por el Consejo Directivo la NTC-ISO/IEC 27001. Esta norma es una adopción idéntica (IDT) por traducción, respecto a su documento de referencia, la norma ISO/IEC 27001.

- En julio de 2007 se emite la norma NTC-ISO/IEC 27002 que es el nuevo nombre de la ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- Recientemente, la última edición de 2013 de la ISO/IEC 27002 ha sido actualizada a un total de 14 dominios, 35 objetivos de control y 114 controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. En Colombia aún no se ha actualizado esta norma.

10.18.2 La evolución de las normas

La ISO desarrolla una familia de normas para el SGSI, cuyo contenido incluye los requisitos para estos tipos de sistemas, gestión del riesgo, métricos y medidos de seguridad de la información y las directrices para la aplicación. La denominación que se utilizará es la ISO/IEC JTC 1/SC 27, que se publicará en secuencia, utilizando el número de serie 27000.

En 2005, se aprobó la 27001 versión colombiana NTC ISO/IEC 27001, que tiene la siguiente nomenclatura: ISO/IEC 27001:2005. Tecnología de la información. Sistema de gestión de seguridad de la información.

Actualmente, para el área de seguridad de la información están publicadas por la ISO o por ICONTEC, las siguientes normas:

- ICONTEC NTC ISO/IEC 27001:2005. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Esta norma es una adopción idéntica (IDT) por traducción, respecto a su documento de referencia, la norma ISO/IEC 27001.
- ICONTEC NTC ISO/IEC 27002:2007. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. Es el nuevo nombre de la ISO 17799:2005, manteniendo 2005 como año de edición.
- ICONTEC NTC 5411-1:2006. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones.
- ICONTEC GTC 169:2008. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.

» ICONTEC NTC 5722:2009. Gestión de la continuidad del negocio. Requisitos.
» ICONTEC GTC 176:2010. Guía para la gestión de la continuidad del negocio (GCN).
» ISO/IEC 27000:2009 - *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*
» ISO/IEC 27004:2009 *covers information security management measurement (metrics).*
» ISO/IEC 27003:2010 *Information technology. Security techniques. Information security management system implementation guidance*
» ISO/IEC 27005:2011 *covers information security risk management.*
» ISO/IEC 27006:2011 *Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.*
» ISO/IEC 27007:2011 *is a guide to auditing Information Security Management Systems.*
» ISO/IEC TR 27008:2011 *Information technology. Security techniques. Guidelines for auditors on information security controls.*
» ISO/IEC 27010:2012. *Information technology. Security techniques. Information security management for inter-sector and inter-organizational communications.*
» ISO/IEC 27032:2012. *Information technology. Security techniques. Guidelines for cybersecurity.*
» ISO/IEC 27033-2:2012. *Information technology. Security techniques. Network security - Part 2: Guidelines for the design and implementation of network security.*
» ISO/IEC 27034-1:2011. *Information technology. Security techniques. Application security - Part 1: Overview and concepts.*
» *ISO/IEC 27035:2011. Information technology. Security techniques. Information security incident management.*
» ISO/IEC 18028-4:2005. *Information technology. Security techniques. IT network security- Part 4: Securing remote access.*
» ISO/IEC 18028-5:2006. *Information technology. Security techniques. IT network security. Part 5: Securing communications across networks using virtual private networks.*
» ISO/IEC 18033-4:2011. *Information technology. Security techniques. Encryption algorithms. Part 4: Stream ciphers.*
» ISO/IEC 29192-1:2012. *Information technology. Security techniques. Lightweight cryptography - Part 1: General.*
» ISO/IEC 29192-2:2012. *Information technology. Security techniques. Lightweight cryptography - Part 2: Block ciphers.*
» ISO/IEC 11770-5:2011. *Information technology. Security techni-*

ques. Key management - Part 5: Group key management.

- ISO/IEC 24760-1:2011. *Information technology. Security techniques. A framework for identity management - Part 1: Terminology and concepts.*
- ISO/IEC 29128:2011. *Information technology. Security techniques. Verification of cryptographic protocols.*
- ISO/IEC 29100:2011. *Information technology. Security techniques. Privacy framework.*
- ISO 22320:2011. *Societal security. Emergency management. Requirements for incident response.*
- ISO 22301:2012. *Societal security. Business continuity management systems. Requirements*
- ISO/IEC 27001:2013. *Is the Information Security Management System (ISMS) requirements standard, a formal specification for an ISMS.*
- ISO/IEC 27002:2013. *Is the code of practice for information security controls describing good practice information security control objectives and controls.*
- ISO/IEC TR 27016:2014. *IT Security. Security techniques. Information security management. Organizational economics.* Fue publicada como un reporte técnico más que un estándar internacional complete.

10.18.3 Seguridad de la información en la administración pública en Colombia

Ley 1273 del 5 de enero de 2009 (Delito Electrónico en Colombia), por medio de la cual se modifica el Código Penal colombiano, se crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

A mediados de 2009 en el gobierno del ex presidente Álvaro Uribe Vélez se sanciona la Ley 1341 por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones, TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones, pasando del Ministerio de Comunicaciones al actual Ministerio de Tecnologías de la Información y las Comunicaciones.

Con esta Ley se enmarca el desarrollo del sector y se promueve el acceso y uso de las TICs a través de la masificación, el impulso a la libre

competencia, el uso eficiente de la infraestructura y en especial, busca fortalecer la protección de los derechos de los usuarios.

El documento CONPES 3650 del 15 de marzo de 2010 declara de importancia estructural la implementación de la "Estrategia de Gobierno en Línea en Colombia" y exhorta al Ministerio de Tecnologías de la Información y las Comunicaciones, con el apoyo del Departamento Nacional de Planeación, a formular los lineamientos de política que contribuyan a la sostenibilidad de la "Estrategia de Gobierno en Línea".

El artículo 64 de la Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, establece que el gobierno nacional establecerá los estándares y protocolos que deberán cumplir las autoridades para incorporar en forma gradual la aplicación de medios electrónicos en los procedimientos administrativos;

El artículo 227 de la Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo 2010-2014, señala que para el ejercicio de sus competencias las entidades públicas y los particulares que cumplen con funciones públicas deberán poner a disposición de la Administración Pública, bases de datos de acceso permanente y gratuito con la información que producen y administran. De igual forma, el parágrafo 3 del mismo artículo señala que el Gobierno Nacional debe garantizar, mediante la implementación de sistemas de gestión para la seguridad de la información, que el acceso a las bases de datos y la utilización de la información sean seguros y confiables para no permitir su uso indebido; El artículo 230 de la Ley 1450 de 2011 establece que todas las entidades de la Administración Pública deberán adelantar las acciones señaladas en la "Estrategia de Gobierno en Línea", liderada por Ministerio de Tecnologías de la Información y las Comunicaciones, a través del cumplimiento de los criterios que éste establezca;

El artículo 232 de la Ley 1450 de 2011 prevé que los organismos y entidades de la Rama Ejecutiva de los órdenes nacional y territorial deberán racionalizar sus procesos, procedimientos, trámites y servicios internos, haciendo uso de las tecnologías de la información y las comunicaciones, con el propósito de ofrecer una oportuna, eficiente y eficaz prestación del servicio en la gestión de las organizaciones;

La Ley 1474 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, hace referencia al uso obligatorio de los sitios web de las entidades públicas como mecanismo obligatorio para la divulgación de información pública;

El Decreto–Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, hace referencia al uso de medios electrónicos como elemento necesario en la optimización de los trámites ante la Administración Pública y establece en el artículo 4º que las autoridades deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas

La Ley 1581 del 17 de octubre 2012 de protección de datos personales es sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional. Como resultado de la sanción de la Ley 1581, toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

El Decreto 2963 de 2012 firmado el 21 de diciembre de 2012, por el cual se establecen los lineamientos generales de la "Estrategia de Gobierno en Línea de la República de Colombia", se reglamentan parcialmente las Leyes 1437 de 2011 y 1450 de 2011, y se dictan otras disposiciones.

Para proteger a los ciudadanos de los riesgos informáticos, el gobierno colombiano creó tres dependencias:

- Mediante la Circular Interna 0335 del 1 de Septiembre de 2011, el Ministerio de Defensa Nacional creó el ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), encargado de coordinar a escala nacional los aspectos de ciberseguridad.
- El Comando Conjunto Cibernético de las Fuerzas Militares, que tiene la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.
- El Centro Cibernético Policial, que está a cargo de la prevención, la investigación y apoyo en la judicialización de los delitos informáticos. Para ello, cuenta con un comando de Atención Inmediata Virtual (CAI Virtual) para recibir las denuncias de los ciudadanos.

10.18.4 El cumplimiento de las políticas y normas

Recuerde que la información de seguridad debe revisarse periódicamente y el análisis debe basarse en políticas y normas en uso. Por lo tanto, las organizaciones deben garantizar el cumplimiento de las políticas y normas para la seguridad de la información.

Como se sabe, la política de seguridad de una organización establece reglas que deben seguirse para garantizar la seguridad de sus activos. Además, existen normas que ayudan a las organizaciones en esta tarea. Por lo tanto, las organizaciones deben asegurarse de que sus sistemas estén de acuerdo con las políticas y normas para garantizar la seguridad de la información, dado que la seguridad es un aspecto a ser analizado periódicamente y con base en las políticas empleadas. En particular, la norma NTC-ISO/IEC 27002:2007 recomienda que los sistemas de información deben ser auditados siguiendo las normas implantadas de la seguridad de la información.

10.18.5 Subsanando las no conformidades de trabajo

Al encontrar una no conformidad durante el proceso de verificación del cumplimiento de las políticas y normas de seguridad, la norma NTC-ISO/IEC 27002:2007 recomienda:

- Determinar las causas de no conformidad.
- Evaluar la necesidad de acciones para no repetir la no conformidad.
- Aplicar medidas correctivas.
- Analizar las medidas correctivas aplicadas.

También es importante mantener registros de todos los resultados obtenidos en las anteriores recomendaciones.

10.18.6 Conformidad técnica

En las organizaciones, es importante llevar a cabo la verificación periódica de la conformidad de sus sistemas de información con las normas de seguridad de la información aplicadas.

Para este propósito, se puede utilizar, por ejemplo, pruebas de penetración previamente planificada, durante los cuales se documentan los resultados con la posibilidad de repetir tantas veces como sea necesario. La verificación de la conformidad técnica se puede hacer:

- Manualmente, con la ayuda de herramientas de apoyo;
- Por un especialista, con la ayuda de herramientas automatizadas para la generación de un informe técnico.

Ejemplos de las recomendaciones para el cumplimiento:

- Código de ética y conducta profesional.
- Utilizando un modelo apropiado de identidad digital.
- Alertar adecuadamente sobre el monitoreo en el entorno electrónico.
- Actualizar los contratos que implican cláusulas sobre la seguridad de la información.
- Definir y publicar políticas objetivas y claras.
- La política de la seguridad de la información debe ser actualizada, clara y objetiva.

A continuación se presentan algunos ejemplos de recomendación general relativa a la atención acerca de la conformidad con las políticas y normas de la seguridad de la información:

- Definición de un código de ética y conducta profesional, tratando los aspectos de tecnología y de información;
- Definición de un modelo técnico-legal de identidad digital donde se puede, por ejemplo, especificar el uso de claves y certificados digitales, entre otros;
- Cuidados adecuados con avisos de monitoreo del entorno en términos de la red, los servicios de Internet, entre otros;
- Mantenimiento de contratos con cláusulas sobre la seguridad de la información, observando controles, auditorías, derechos de propiedad intelectual, etc;
- Definición formal y la publicación de las políticas, tanto internas como externas a la organización.

Ejercicio de refuerzo - conformidad técnica

- Explique qué es conformidad técnica

10.19 Auditoría de sistemas de información

En cuanto a las consideraciones relativas a la auditoría, se presentarán los siguientes subtemas:

- Auditoría, mostrando las principales necesidades de protección de las herramientas utilizadas por el proceso en las organizaciones.
- Cuidados durante la auditoría, alertando sobre algunas de las preocupaciones relevantes de un proceso adecuado de auditoría en la organización con el fin de garantizar su conformidad con las leyes, políticas y normas vigentes.

Durante la auditoría de sistemas de información, se recomienda proteger los sistemas y herramientas empleados, asegurando su integridad y el control del acceso no autorizado. Por lo tanto, las actividades de auditoría deben ser realizadas según un planeamiento adecuado, y de acuerdo común con los líderes de la organización, a fin de no influir en su negocio.

El acceso a las herramientas de auditoría debe ser controlado, y se debe almacenar en lugares separados o aislados.

10.20 El cuidado en la auditoría

La auditoría debe llevarse a cabo después del acuerdo formal con los líderes de la organización. Todas las verificaciones de cumplimiento deben ser ejecutadas según el acuerdo formal establecido, y debidamente controladas. En particular, se recomienda que la verificación sea limitada a solo lectura y sólo cuando sea necesario el acceso, deben ser generadas copias para su uso. Estas copias deberán ser aisladas y almacenadas de forma segura o eliminadas al final de la auditoría. Los recursos deben ser identificados únicamente en la organización para, de este modo, ponerlos a disposición de la auditoría. Todos los accesos deben ser controlados; es decir, monitoreados y registrados. Finalmente, todo el proceso debe ser documentado.

10.21 Otras normas relevantes

Control Objectives for Information Technologies, CobiT 4.1, es un marco de gobierno de las TI, que incluye buenas prácticas para el control de requisitos, mapas de auditoría, cuestiones técnicas y riesgos empresariales; consiste de cuatro dominios: *Plan and organize, Acquire and implement, Deliver and support and Monitor and evaluate.*

Se recomienda el uso de CobiT como medio para optimizar las inversiones en TI, maximizando el ROI (en inglés *Return on Investments*) y proporcionando métricas para evaluar los resultados.

En los dominios de CobiT se hace énfasis en la seguridad, por ejemplo, en el proceso: definir el proceso de arquitectura de información del dominio: Planear y Organizar, PO, existe el esquema de clasificación de datos y los niveles de seguridad.

CobiT 5 fue lanzado en abril de 2012, como la consolidación e integración del CobiT 4.1, Val IT 2.0 y Risk IT 2.0. Se alinea con estructuras y estándares como *Information Technology Infrastructure Library*, ITIL, *International Organization for Standardization*, ISO, Project *Management Body of Knowledge* , PMBOK, PRINCE2 y *The Open Group Architecture Framework*, TOGAF. Esta versión incorpora las últimas novedades en gobierno corporativo y tecnicas de gestión.

Navegue en Cobit Publications and Downloads: www.isaca.org/cobit.
ITIL comprende una librería de buenas prácticas (políticas, procesos, procedimientos e instrucciones de trabajo) para la gestión de las TI de dominio público, centrado en el cliente y en la calidad de los servicios de las TI y el establecimiento de un conjunto de procesos y procedimientos de gestión organizados en disciplinas.Se convirtió en el estándar BS 15000 siguiendo la estructura de ISO 9000:2000.

En particular, el Operations Level Agreement, OLA y el Service Level Agreement, SLA, son parte del proceso de ITIL de seguridad de la información, que cubre información tales como métodos de acceso permitido, acuerdos en relación con la auditoría y el registro, medidas seguridad física, entrenamiento a los usuarios, los procedimientos de autorización de usuarios y disposiciones para informar e investigar los incidentes de seguridad.

10.22 Otras leyes pertinentes

- Ley 565 del 2 de febrero de 2000, por medio de la cual se aprueba el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor, adoptado en Ginebra, el 20 de diciembre de 1996.
- Resolución 270 del 4 de marzo de 2000, por la cual se dictan normas sobre protección a los usuarios para la prestación de servicios públicos no domiciliarios de telecomunicaciones.
- Acción pública de inconstitucionalidad contra la Ley 527 sobre mensajes de datos, comercio electrónico y firma digital de 8 de junio de 2000.
- Ley 594 de 4 de julio de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones (Diario Oficial nº 44084 de 14 de julio de 2000).
- Decreto 1747 de 11 de septiembre de 2000, por el cual se reglamenta parcialmente la Ley 527 certificados y firmas digitales.
- Resolución 7652 de 22 de septiembre de 2000, de la Dirección General de Impuestos y Aduanas Nacionales, por la cual se reglamenta la administración, publicación y uso de la información electrónica vía INTRANET e INTERNET en la Dirección de Impuestos y Aduanas Nacionales.
- Resolución 307 del 2 de octubre de 2000, de la Comisión de Regulación de Telecomunicaciones, por la cual se promueve el acceso a Internet a través de planes tarifarios para el servicio de TPBCL y se dictan otras disposiciones
- Ley 679 del 3 de agosto de 2001 sobre Abuso y pornografía de menores en internet. (Diario Oficial número 44509 del 4 de agosto de 2001).
- Radicación 1376 del Consejo de Estado del 11 de diciembre de 2001 sobre Nombres de Dominio.
- Decreto 25 del 11 de enero de 2002 del Ministerio de Comunicaciones, por el cual se adoptan los Planes Técnicos Básicos y se dictan otras disposiciones.
- Decreto 55 del 15 de febrero de 2002 de la Alcaldía Mayor de Bogotá, por medio del cual se establece "El Sistema de Declaración y Pago de Impuestos Distritales a través de medios electrónicos".
- Resolución 20 del 14 de enero de 2003, del Ministerio de Comunicaciones, por medio de la cual se establece el procedimiento a seguir por el Ministerio de Comunicaciones para la fijación de las condiciones de administración del dominio.co.
- Decreto 600 del 14 de marzo de 2003, por medio del cual se expiden normas sobre los servicios de valor agregado y telemáticos y se reglamente el Decreto-Ley 1900 de 1990.

- Ley 892 del 7 de julio 2004. Voto electrónico
- Resolución 1455 del 5 de septiembre de 2003, del Ministerio de Comunicaciones, por medio de la cual se regula la administración de registros del dominio.co
- Ley 1065 del 29 de julio de 2006, por la cual se define la administración de registros de nombres de dominio.co y se dictan otras disposiciones (Diario Oficial nº 46.344 de 29 julio de 2006). (Derogada por el artículo 73 de la Ley 1341 de 2009)
- Decreto 4540 del 22 de diciembre de 2006, por medio del cual se adoptan controles en aduana, para proteger la Propiedad Intelectual.
- Acuerdo 279 del 29 de marzo de 2007, del Consejo de Bogotá, por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
- Decreto 2870 del 31 de julio de 2007, por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones. (Diario oficial nº 46.706 del 31 de julio de 2007).
- Resolución 284 del Ministerio de Comunicaciones del 21 de febrero de 2008, por la cual adopta el modelo operativo para la administración del dominio.co
- Decreto 1151 del Ministerio de Comunicaciones, del 14 de abril de 2008, mediante el cual se establecen los lineamientos generales de la "Estrategia de Gobierno en Línea de la República de Colombia", se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
- Ley 1221 del 16 de julio de 2008, por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones (Diario Oficial nº 47.052).
- Ley 1245 del 6 de octubre de 2008, por medio de la cual se establece la obligación de implementar la portabilidad numérica y se dictan otras disposiciones.
- Ley 1266 del 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Diario Oficial nº 47.219).
- Decreto 1727 del 15 de mayo de 2009, del Ministerio de Hacienda y Crédito Público, por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información. (Diario Oficial nº 47.350 de 15 de mayo de 2009).

- Resolución 244 del 30 de julio de 2009, por la cual se establece el Sistema de Información Automático de Registro de Obras, Fonogramas y Contratos, en la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, y se determinan las condiciones de uso de dicho sistema. (Diario Oficial nº 47.446 de 19 de agosto de 2009).
- Resolución 2229 del 28 de octubre de 2009 CRC, de la Comisión de Regulación de las Comunicaciones, de creación del Registro de Números Excluidos, aplicado al SPAM telefónico.
- Resolución 2239 del 24 de noviembre de 2009 CRC, de la Comisión de Regulación de las Comunicaciones, Localización e identificación de personas y medidas de acceso a los CAE para personas con discapacidad.
- Resolución 2251 del 11 de diciembre de 2009 CRC, de la Comisión de Regulación de las Comunicaciones, por la cual se modifica la Resolución 1914 de 2008 de la CRT.
- Resolución 2347 del 26 de enero de 2010 CRC, de la Comisión de Regulación de las Comunicaciones, con la que se establecen disposiciones en materia de protección de los derechos de usuarios respecto de tarifas de telefonía pública básica conmutada.
- Resolución 2353 del 29 de enero de 2010 CRC, de la Comisión de Regulación de las Comunicaciones, por la cual se establece la metodología para la medición del Nivel de Satisfacción del Usuario de los Servicios de TRBCL y TRBCLE. Además se recoge el procedimiento para el cálculo del Factor de Calidad.
- Resolución 202 del 8 de marzo de 2010, del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se expide el glosario de definiciones conforme a lo ordenado por el inciso segundo del artículo 6 de la Ley 1341 de 2009. (Diario Oficial nº 47.656 de 19 de marzo de 2010).
- Decreto 1162 del 13 de abril de 2010, por el cual se organiza el Sistema Administrativo Nacional de Propiedad Intelectual y se crea la Comisión Intersectorial de Propiedad Intelectual.
- Resolución 2533 del 30 de abril de 2010 CRC, de la Comisión de Regulación de las Comunicaciones, que modifica la normativa aplicable a la portabilidad numérica.

Capítulo

11

Cuaderno de actividades

11.1 Guía de actividades 1

Actividad 1 - Identificación de los ataques

Para cada situación, a continuación, indicar el modelo de ataque aplicable. Justifique su respuesta:

Tabla 13. Ejercicio identificación de los ataques

Situación	Modelo de ataque	Justificación
Adición de un registro falso en la base de datos		
Deshabilitar un sistema de archivos		
Modificación de los datos que viajan por la red		
La destrucción física de un componente de hardware		
Captura de datos de la red, mediante espías		
Modificación de un programa para que se ejecute de manera diferente		

Actividad 2 - Identificando vulnerabilidades

Para cada una de las situaciones a continuación, citar al menos una vulnerabilidad posible que pueda ser explotada para materializar una amenaza a la seguridad de la información de una organización. Justifique su respuesta.

1. El personal de servicios de mensajería diariamente realiza la recolección y entrega de mensajes.

2. Los ex empleados que dejaron la organización porque fueron despedidos.

3. Empleado que viaja al servicio de la organización y accede a la red de forma remota

4. Uso de *notebook* personal sin registro en la lista de activos.

5. Computador de trabajo conectado al sistema sin que el usuario esté cerca.

Actividad 3 – Identificando la forma de ataque

Identifique la forma de ataque aplicable a cada situación a continuación. Justifique su respuesta:

1. Captura y acceso a un archivo transferido desde un cliente a un servidor a través de la red.

2. Alteración de parte de un mensaje legítimo.

3. Análisis del tráfico de una red utilizando un *sniffer*.

4. Una interrupción de la red, debido a una congestión de tráfico que ha degradado su rendimiento.

5. Uso del nombre de usuario y la contraseña de otro usuario.

Actividad 4 – La asociación de las categorías de servicios de seguridad

Para cada contexto que se presenta a continuación indique el servicio (s) directamente asociado (s):

1. Mantenimiento de información secreta, realizado por medio de códigos de transmisión de la red

2. Redundancia de servidores de misión crítica

3. No abrir archivos o ejecutar programas adjuntos a mensajes de correo electrónico sin verificarlos primero con un antivirus

4. Los usuarios deben declarar por qué necesitan cambios en sus privilegios en la organización y cómo se relaciona la solicitud con las actividades desempeñadas por ellos

5. Se prohíbe a los usuarios el derecho de modificar, eliminar o copiar los archivos que pertenecen a otro usuario sin su permiso expreso

Actividad 5 – Caso de estudio: su organización

Teniendo en cuenta su organización actual, haga un rápido análisis de la situación de la seguridad de la información y responda:

1. ¿Cuáles son los controles que desde el punto de vista legal y las mejores prácticas necesita su organización? Justifique

2. ¿Cuáles son los factores críticos de éxito de seguridad de la información en su organización?

11.2 Guía de actividades 2

Actividad 1 – Conocer la norma ISO/IEC 27002:2007

1. Citar y explicar la categoría principal de seguridad de la información de la norma ISO/IEC 27002:2007 que se refiere a la seguridad física.

2. Durante el análisis de la información acerca de la seguridad de la información de su institución no fue identificada la existencia de ninguna política de seguridad de la información. Cite y explique la categoría principal de seguridad de la información de la norma ISO/IEC 27002:2007 que se refiere a la política de seguridad.

3. ¿Cómo está estructurada cada categoría de control?

Actividad 2 – Entendiendo la norma NTC ISO/IEC 27002:2007

1. ¿Cuál es el objetivo de control de la categoría 10.1 (procedimientos y responsabilidades operacionales)?

2. Describa el control 6.1.2 (Coordinación de la seguridad de la información).

3. Explique las directrices para la implementación del control 11.5.5 (límite de tiempo de sesión).

4. Describa la información adicional para 15.1.5 (Prevención del uso indebido de los recursos de procesamiento de la información).

Actividad 3 – Trabajando con la norma NTC ISO/IEC 27002:2007

Durante el trabajo para implementar un sistema de gestión de seguridad de la información, cuando se realizaba el análisis de riesgo, se identificaron varias vulnerabilidades, que se presentan en la siguiente tabla. Con base en la norma ISO/IEC 27002:2007, indique el control o los controles de la norma que se deben implementar para abordar cada una de estas vulnerabilidades. Como ejemplo está la respuesta a la primera vulnerabilidad.

Tabla 14. Ejercicio norma NTC ISO/IEC 27002:2007

No.	Vulnerabilidad	Control(s) n° (s)
1	Protección física (puerta) de acceso a la sala de servidores inadecuada.	9.1.2 + 9.2.1 + 14.1.1
2	Red eléctrica inestable.	
3	Control de reclutamiento inadecuado de mano de obra.	
4	La falta de conciencia de seguridad.	
5	Almacenamiento inadecuado de copia de seguridad.	
6	Falta de control de cambio en el desarrollo de software.	
7	Transferencia de claves y contraseñas en texto plano	
8	Documentos almacenados en local sin protección.	
9	Documentos clasificados expuestos sobre la mesa.	
10	Falta de protección contra virus y código malicioso.	
11	El uso de los datos de producción para pruebas de software en desarrollo.	
12	Control inadecuado/inexistente para llevar a cabo el trabajo remoto.	
13	Control inapropiado de los servicios externalizados.	
14	Falta de procedimiento para la remoción de los equipos para mantenimiento.	
15	Falta de planificación de pruebas de los planes de continuidad	
16	Empleado utilizando recursos computacionales para uso personal (Descarga de películas y música)	
17	La misma contraseña es utilizada por varios usuarios.	
18	No fueron identificados sistemas o procedimientos para la entrada física en áreas seguras	
19	No existe un procedimiento para la clasificación de la información	
20	El funcionario que controla los servidores de aplicaciones desconocía el procedimiento en caso de eventos de seguridad.	

Actividad 4 – Caso de estudio: su organización

Teniendo en cuenta las respuestas dadas para su organización en el estudio de caso de la guía de actividades anteriores, analice la situación de la organización de acuerdo con las secciones de la norma y responda:

1. ¿Qué secciones de la norma ya se implementaron plenamente en su organización? ¿Cuáles están parcialmente implementadas? Justifique.

2. ¿Cuáles secciones son extremadamente necesarias, de acuerdo con el negocio de su organización? Justifique.

3. ¿Cómo justificaría usted la necesidad de utilizar la norma e implementar sus controles? Justifique.

11.3 Guía de actividades 3

Actividad 1 – Conociendo el ciclo PHVA

Describa las principales actividades de un SGSI en cada etapa del ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Actividad 2 – Identificando requisitos del SGSI

Enumere los requisitos que, según la norma, deben ser incluidos obligatoriamente en el establecimiento de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Actividad 3 – Establecimiento y operación del SGSI

1. ¿Cuáles son las ocho actividades obligatorias que una organización debe realizar para implementar un SGSI?

2. ¿Qué actividad debe ser implementada por la organización para sus recursos humanos? Justifique su respuesta.

Actividad 4 – Monitoreando y analizando el SGSI

Después de leer los puntos 4.2.3 y 4.2.4 de la norma, explique lo que significa "análisis crítico" y su importancia.

Actividad 5 –Documentando el SGSI

1. ¿Cuáles son los documentos que deben incluirse en el SGSI?
2. ¿Qué es la Declaración de Aplicabilidad?

Actividad 6 – Implementando el SGSI en la institución

1. Teniendo en cuenta el estado actual de la seguridad de la información en su institución, presente las etapas mínimas y necesarias para que la implementación del SGSI ocurra en el plazo de un año. Indique los plazos a tener en cuenta en cada etapa.

2. De acuerdo a su anterior respuesta, cite secuencialmente los documentos requeridos

11.4 Guía de actividades 4

Actividad 1 - Comprendiendo la política de seguridad de la información

1. De acuerdo con la ISO/IEC 27002:2007, ¿cuál es el objetivo de control de la política de seguridad de la información?

2. De acuerdo con la NTC ISO/IEC 27002:2007, ¿cuáles son las directrices para la aplicación de una política de seguridad?

Actividad 2 – Elaborando una política de seguridad de la información

1. Usted fue designado(a) para presentar una propuesta de política de seguridad para el servicio de correo electrónico en su institución. Describa y justifique las etapas que adoptará para concluir la propuesta:

2. ¿Quién tiene que aprobar su propuesta? Justifique su respuesta.

Actividad 3 – Implementando una política de seguridad

¿Cuál es la actividad esencial después de la finalización y aprobación de la política? Presente su justificación.

Actividad 4 - Desarrollar una política de seguridad para su organización

Como jefe del departamento de las TI, fue designado(a) para hacer parte del Comité de Seguridad de la Información de su organización. El comité está actualmente haciendo una revisión de algunos textos de la política de seguridad.

1. Analice el siguiente texto de la política, señale los errores existentes y escríbalo de nuevo:

a. Los usuarios no deben utilizar los clientes de *Internet Service Provider*, ISP, y líneas *dial-up* para acceder a internet con los computadores de la organización X. Toda la actividad de acceso a internet debe pasar a través de los *firewalls* de la organización X de modo que los controles de acceso y mecanismos de seguridad se puedan aplicar.

b. Un documento que contiene información clasificada como secreta o altamente confidencial nunca puede ser enviado a una impresora de red sin que allá esté una persona autorizada para proteger su confidencialidad durante y después de la impresión.

c. Los generadores de energía secundarios y de respaldo deben ser empleados cuando sea necesario para garantizar la continuidad del servicio durante fallas o cortes de energía.

2. En una reunión de comité se le solicitó como especialista en el tema, que presentase cuáles deberían ser las primeras políticas de seguridad que se deben trabajar y desarrollar. ¿Cuál es su respuesta? Justifique

11.5 Guía de actividades 5

Actividad 1 – Comprender los conceptos de gestión del riesgo

Presente en el cuadro los conceptos de gestión del riesgo y cite ejemplos de cada fase:

Tabla 15. Conceptos de gestión del riesgo

Fase	Concepto	Ejemplo
Análisis del riesgo		
La evaluación de riesgos		
Aceptación de riesgos		
El tratamiento del riesgo		
La comunicación del riesgo		

Actividad 2 – Realizando la gestión del riesgo

1. Explicar lo que es un análisis de impacto.

2. ¿Cómo se calcula el riesgo? Justifique.

3. ¿Cuáles son los métodos de evaluación de los riesgos existentes?

4. Describir lo que significa "tratar el riesgo".

Actividad 3 – Realizando la gestión del riesgo

1. Describir las actividades que se desarrollan en su organización para llevar a cabo el análisis de riesgos. ¿Cuáles son los objetivos de este análisis?

2. Teniendo en cuenta las actividades anteriores desarrolladas, analice un servidor de aplicaciones (o el proceso de control de acceso físico) de la organización indicando lo que se pide.

   a. 03 (tres) amenazas

   b. 06 (seis) vulnerabilidades.

   c. Probabilidad de cada vulnerabilidad sea explotada (Alto, Medio, Bajo).

   d. La criticidad del activo para los negocios de la organización (Alta, Media, Baja).

   e. Impacto para cada que cada vulnerabilidad sea explotada y se materialice una amenaza (Alta, Media, Baja).

   f. Riesgo del activo considerado (Utilice los procesos, los parámetros y el cálculo del ejemplo anterior).

Actividad 4 – Realizando la gestión del riesgo en su organización.

1. Presente las necesidades de gestión del riesgo para su organización. Justifique su respuesta

2. Escriba un alcance inicial y relacione dos profesionales para conformar el equipo de análisis. Justifique su respuesta.

11.6 Guía de actividades 6

Actividad 1 – Seguridad de la información en la gestión de operaciones comunicaciones

Usted ha sido asignado para desempeñar las funciones de gestión de operaciones y comunicaciones. A continuación se presentan algunas situaciones en las que debe decir lo que se debe hacer y presentar su justificación:

Tabla 16. Seguridad de la información en la gestión de operaciones comunicaciones

No.	Situación	Respuestas/ procedimientos	Justificación
1	Ingreso de un nuevo empleado en la organización, que será usuario del sistema de control financiero de la organización.		
2	La base de datos se corrompió, no había ninguna copia de seguridad.		
3	Un servidor funciona mal y necesita ser llevado a mantenimiento fuera del ambiente del centro de datos.		
4	La gestión de recursos humanos, dijo que ha adquirido un nuevo sistema y ha determinado que debe estar instalado en el servidor de aplicaciones que funciona actualmente.		
5	La gestión de investigación y desarrollo, advirtió que la administración del servidor de aplicaciones, de la base de datos y del control de la versión se llevará a cabo por el mismo investigador		
6	En un estudio realizado por un consultor externo para examinar la madurez en seguridad de la información, hemos identificado varios computadores de profesores que carecen de antivirus instalado.		
7	Ha sido identificada en la división financiera que se produjo un cambio en los archivos, pero no pudieron identificar quién realizó la alteración.		

Actividad 2 – Implementación de seguridad de la información en la gestión de las operaciones y sus comunicaciones de su organización.

Usted sigue siendo miembro del comité de seguridad de la información y debe presentar propuestas para la seguridad de la información en la gerencia de operaciones y comunicaciones de su organización. Elabore para cada uno de los siguientes elementos cinco temas que deben ser cubiertos en cada política:

a. Las copias de seguridad

b. Procedimientos contra software malicioso

c. Tratamiento de medios

d. El procesamiento de los documentos.

e. Seguridad de las redes.

f. Transferencia de información.

11.7 Guía de actividades 7

Actividad 1 – Entender la seguridad de acceso y la seguridad ambiental

Usted fue designado(a) para realizar una evaluación de la seguridad de acceso y la seguridad del entorno de la organización. A continuación se presentan algunas situaciones que fueron encontradas y sobre las que debería decir lo que se debe hacer y presentar su justificación:

Tabla 17. Entender la seguridad de acceso y la seguridad ambiental

No.	Situación	Respuestas/ procedimientos	Justificación
1	Empleados sin identificación (tarjeta de identificación).		
2	Visitantes caminando por la organización sin ningún tipo de identificación o registro de su entrada.		
3	Cuarto del archivo documental sin extintores o un sistema de detección		
4	Los colaboradores tercerizados no realizaron ningún tipo de entrenamiento en seguridad de la información		
5	Se identificó que los ex empleados todavía tenían cuentas de los usuarios de algunos sistemas.		
6	En el área de contabilidad los funcionarios comparten la misma contraseña.		
7	En el área de investigación y desarrollo se identificó que algunos funcionarios de nivel técnico tenían acceso a las áreas restringidas de los investigadores.		

Actividad 2 – Políticas de acceso

1. ¿Qué es lo mínimo que debe aparecer en una política de control de acceso?

2. ¿ Cuáles son los controles de acceso lógico? Y de acceso físico?

3. ¿Cuáles son las categorías existentes de controles de acceso físico? ¿Cuáles son las diferencias entre ellas?

4. Nombre dos amenazas de entorno y sus respectivos controles de entorno.

Actividad 3 – implementando la seguridad de acceso y entorno de su organización

Usted es miembro del comité de seguridad de la información, y debe presentar propuestas relacionadas a la seguridad de la información, específicamente la seguridad de acceso y ambiente de su organización. Así, elabore para cada uno de los siguientes elementos cinco temas que deben ser cubiertos en cada política:

a. Control de acceso lógico.

b. Contraseñas.

c. Acceso fisico.

d. Controles de entorno.

e. Seguridad de recursos humanos.

11.8 Guía de actividades 8

Actividad 1 –Comprendiendo la seguridad organizacional

1. Explique la importancia de la asignación de responsabilidades para la seguridad de la información en su organización.

2. ¿Cómo y dónde debe actuar la coordinación de seguridad de la información?

Actividad 2 – Realizando la seguridad organizacional

1. Describa cómo debe ser tratado y ejecutado el inventario de los bienes.

2. Explique la razón de la diferencia de tratamiento de los recursos y la información a disposición de terceros. Presente un ejemplo práctico de su organización

3. Describa los procedimientos que deben adoptarse en el trato con los clientes.

4. Nombre dos ejemplos prácticos para la gestión de servicios de terceros.

Actividad 3 – Implementando la seguridad organizacional

Usted sigue siendo miembro del comité de seguridad de la información y debe presentar algunas propuestas para la seguridad de la información en la seguridad organizacional de su organización. Así, prepare para cada uno de los siguientes elementos cinco aspectos que deben ser abordados en cada política:

a. Activos.

b. Terceros proveedores de servicios en el área de TI.

c. Terceros proveedores de servicios en el área de servicios generales.

d. Los proveedores de equipos de oficina.

e. Clientes.

f. Acuerdos.

g. Responsabilidades en materia de seguridad de la información.

Guía de actividades 9

Actividad 1 – Comprendiendo los conceptos de la gestión de continuidad del negocio

1. Explicar qué es la gestión de la continuidad del negocio.

2. ¿Qué consideraciones deben abordarse en el tratamiento de la seguridad de la información en el contexto de la continuidad del negocio?

Actividad 2 – Ejecutando la continuidad del negocio

1. Cuál es la estructura mínima de un Plan de Continuidad del Negocio, PCN?

2. ¿Qué debe contemplar la gestión de incidentes de seguridad?

3. ¿Cuál es la importancia de la notificación de los eventos adversos?

4. ¿Cuáles deben ser los procedimientos de gestión de incidentes de seguridad?

5. Describa lo que se debe hacer durante el análisis del impacto en las fases de planeación de contingencias.

6. Explique qué es el "tiempo de recuperación", y utilizando un ejemplo práctico, indique cómo se debe emplear.

Actividad 3 – Ejecutando la continuidad del negocio y la gestión de incidentes en su organización

1. Como miembro del comité de seguridad de la información, usted fue designado para presentar un Plan de Continuidad del Negocio, PCN, para su organización. Durante la presentación del tema, teniendo en cuenta la estructura actual y los objetivos de su institución, ¿qué actividades deben enumerarse para desarrollar este plan?

2. Usted tomó la responsabilidad de la estructuración de un equipo de Tratamiento y Respuestas a Incidentes con las Redes Informáticas, ETIR para su organización. ¿Cómo va estructurar este equipo? Qué profesionales de su organización van a integrar el ETIR? ¿Cuáles son los objetivos del ETIR?

11.10 Guía de actividades 10

Actividad 1 – Entendiendo la legislación

1. En la sociedad digital moderna, ¿es posible equilibrar la seguridad, la privacidad y funcionalidad al mismo tiempo? Explique su punto de vista.

Actividad 2 – La realización del cumplimiento

1. Cite y explique, al menos, dos cuidados con la propiedad intelectual citados en las normas ISO/IEC 27001 y 27002.

2. ¿Qué cuidados se deben tener para la protección de los registros de la organización?

3. ¿Qué cuidados debe tener su organización durante la realización de una auditoría?

Actividad 3 – Realización del cumplimiento en la organización

1. Como miembro del comité de seguridad de la información, usted resuelve presentar un plan para la verificación del cumplimiento de su organización. Teniendo en cuenta la actual estructura y objetivos de su institución, ¿cuáles son las leyes que su institución debe seguir?

2. ¿Cómo va a estructurar un proceso para que su institución esté en conformidad con las leyes específicas de seguridad de la información? ¿Cuáles deberán ser los objetivos de este trabajo?

Capítulo

12

Anexo

12.1 Anexo 1

Tipo	Fecha	Objeto	Link
Ley 1581 de 2012	17 de octubre de 2012	Por el cual se dictan disposiciones generales para la Protección de Datos Personales	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
Ley 1507 de 2012	10 de enero de 2012	"Por la cual se establece la distribución de competencias entre las entidades del estado en materia de televisión y se dictan otras disposiciones".	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45327
Ley 1480 de 2011	12 de octubre de 2011	Por medio de la cual se expide el estatuto del consumidor y se dictan otras disposiciones	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=44306
Ley 1474 de 2011	12 de julio de 2011	"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292
Ley 1437 de 2011	18 de enero de 2011	"Por medio de la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo".	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249
Ley 1450 de 2011	16 de junio de 2011	"Por la cual se expide el Plan Nacional de Desarrollo 2010-2014"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101
Ley 1341 de 2009	30 de julio de 2009	"Por la cual se definen principios y conceptos sobre la Sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones -TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913
Ley 1273 de 2009	5 de enero de 2009	"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Tipo	Fecha	Objeto	Link
Ley 1266 de 2008	31 de diciembre de 2008	"Por la cual se dictan las disposiciones generales del *hábeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
Ley 1150 de 2007	16 de julio de 2007	"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=25678
Ley 1065 de 2006	29 de julio de 2006	Por la cual se define la administración de registros de nombres de dominio.co y se dictan otras disposiciones"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=20867
Ley 970 de 2005	13 de julio de 2005	Por medio de la cual se aprueba la "Convención de las Naciones Unidas contra la Corrupción", adoptada por la Asamblea General de las Naciones Unidas	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17079#0
Ley 962 de 2005	8 de julio de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004
Ley 790 de 2002	27 de diciembre de 2002	"Por la cual se expiden disposiciones para adelantar el programa de renovación de la administración pública y se otorgan unas facultades extraordinarias al Presidente de la República".	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6675
Ley 594 de 2000	14 de julio de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275

Tipo	Fecha	Objeto	Link
Ley 527 de 1999	18 de agosto de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
Ley 489 de 1998	29 de diciembre de 1998	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=186
Ley 190 de 1995	6 de junio de 1995	Por la cual se dictan normas tendientes a preservar la moralidad en la Administración Pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=321
Ley 80 de 1993	28 de octubre de 1993	Por la cual se expide el Estatuto General de Contratación de la Administración Pública	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=304
Ley 57 de 1985	5 de julio de 1985	"Por la cual se ordena la publicidad de los actos y documentos oficiales.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=276
Decreto Ley 019 de 2012	Enero 10 de 2012	"Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45322
Decreto 2618 de 2012	17 de diciembre de 2012	Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones	http://www.mintic.gov.co/index.php/docs-normatividad?pid=58&sid=1009:2618

Tipo	Fecha	Objeto	Link
Decreto 2693 de 2012	21 de diciembre de 2012	Determina los lineamientos que deben seguir las entidades públicas y los particulares que desempeñan funciones públicas en la implementación de la Estrategia de Gobierno en línea en Colombia. Además se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198
Decreto 3443 de 2010	17 de septiembre de 2010	Por el cual se modifica la estructura del Departamento Administrativo de la Presidencia de la República	http://wsp.presidencia.gov.co/Normativa/Decretos/2010/Documents/Septiembre/17/dec344317092010.pdf
Decreto 1630 de 2011	19 de mayo de 2011	"Por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=42907
Decreto 2623 de 2009	13 de julio de 2009	Por el cual se crea el Sistema Nacional de Servicio al Ciudadano.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36842
Decreto 1151 de 2008	14 de abril de 2008	"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones".	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=29774
Decreto 2434 de 2006	18 de julio de 2006	Por el cual se reglamenta la Ley 80 de 1993, se modifica parcialmente el Decreto 2170 de 2002 y se dictan otras disposiciones.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=20708#7
Decreto 4669 de 2005	21 de diciembre de 2005	Por el cual se reglamenta parcialmente la Ley 962 de 2005.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18630
Decreto 3816 de 2003	31 de diciembre de 2003	"Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública"	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=11233

Tipo	Fecha	Objeto	Link
Decreto 2170 de 2002	30 de septiembre de 2002	Por el cual se reglamenta la Ley 80 de 1993, se modifica el decreto 855 de 1994 y se dictan otras disposiciones en aplicación de la Ley 527 de 1999	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5798
Decreto 127 de 2001	19 de enero de 2001	Por el cual se crean las Consejerías y Programas Presidenciales en el Departamento Administrativo de la Presidencia de la República	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/decreto127de2001.pdf
Decreto 1747 de 2000	11 de septiembre de 2000	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277
Decreto Ley 2150 de 1995	5 de diciembre de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1208
Decreto 2893 de 2011	11 de agosto de 2011	Por el cual se modifican los objetivos, la estructura orgánica y funciones del Ministerio del Interior y se integra el Sector Administrativo del Interior	https://www.dnp.gov.co/LinkClick.aspx?fileticket=UY4dJCD-dQY%3D&tabid=1376
Decreto 2674 de 2013	20 de noviembre de 2013	Por el cual se modifica el Decreto número 3355 de 2009.	http://www.cancilleria.gov.co/sites/default/files/Normograma/docs/decreto_2674_2013.htm
Resolución 4914 de 2010	12 de noviembre de 2010	Por la cual se deroga la Resolución 0316 de 2009, se crea y reglamenta el Comité de Gobierno en Línea y Antitrámites del Ministerio de Relaciones Exteriores y de su Fondo Rotatorio.	http://www.cancilleria.gov.co/sites/default/files/Normograma/docs/resolucion_minrelaciones_4914_2010.htm
Decreto 4712 de 2008	15 de diciembre de 2008	Por el cual se modifica la estructura del Ministerio de Hacienda y Crédito Público.	http://www.minhacienda.gov.co/portal/page/portal/HomeMinhacienda/elministerio/Organigrmayestructuraorganica/Decreto%204712%20de%202008%20(Por%20el%20cual%20se%20modifica%20la%20estructura%20del%20Ministerio%20de%20Hacienda%20y%20Cr%E9dito%20P%FAblico).pdf

Tipo	Fecha	Objeto	Link
Decreto 2897 de 2011	11 de agosto de 2011	Por el cual se determinan los objetivos, la estructura orgánica, las funciones del Ministerio de Justicia y del Derecho y se integra el Sector Administrativo de Justicia y del Derecho.	https://www.dnp.gov.co/LinkClick.aspx?fileticket=QfvDSdoE5E8%3D&tabid=1374
Decreto 3570 de 2011	27 de septiembre de 2011	Por el cual se modifican los objetivos y la estructura del Ministerio de Ambiente y Desarrollo Sostenible y se integra el Sector Administrativo de Ambiente y Desarrollo Sostenible.	http://www.minambiente.gov.co/documentos/normativa/ambiente/decreto/dec_3570_270911.pdf
Decreto 3571 de 2011	27 de septiembre de 2011	Por el cual se establecen los objetivos, estructura, funciones del Ministerio de Vivienda, Ciudad y Territorio y se integra el Sector Administrativo de Vivienda, Ciudad y Territorio.	http://www.minvivienda.gov.co/Ministerio/Normativa/Institucional/Normativa/3571%20-%202011.pdf
Decreto 4107 de 2011	2 de noviembre de 2011	Por el cual se determinan los objetivos y la estructura del Ministerio de Salud y Protección Social y se integra el Sector Administrativo de Salud y Protección Social.	http://www.minsalud.gov.co/Normatividad/DECRETO%204107%20DE%202011.pdf
Decreto 4108 de 2011	2 de noviembre de 2011	Por el cual se modifican los objetivos y la estructura del Ministerio del Trabajo y se integra el Sector Administrativo del Trabajo.	https://www.google.com.co/search?q=Decreto+4108+-de+2011&oq=Decreto+4108+-de+2011&aqs=chrome..69i57j0l5.1146j0j4&sourceid=chrome&espv=210&es_sm=122&ie=UTF-8#
Decreto 4890 de 2011	23 de diciembre de 2011	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones	http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/23/dec489023122011.pdf
Decreto 1985 de 2013	21 de diciembre de 2007	Por el cual se modifica la estructura del Ministerio de Agricultura y Desarrollo Rural	https://www.minagricultura.gov.co/Normatividad/Decretos/1985.pdf
Decreto 210 de 2003	Febrero 3 de 2003	Por el cual se determinan los objetivos y la estructura orgánica del Ministerio de Comercio, Industria y Turismo, y se dictan otras disposiciones.	http://www.mincit.gov.co/descargar.php?idFile=7
Decreto 0854 de 2011	23 de marzo de 2011	Por el cual se modifica la estructura del Ministerio de Educación Nacional	http://www.mineducacion.gov.co/1621/articles-267644_archivo_pdf_decreto8545.pdf

Tipo	Fecha	Objeto	Link
Decreto 3517 de 2009	14 de septiembre de 2009	Por el cual se modifica la estructura del Departamento Nacional de Planeación	https://www.dnp.gov.co/LinkClick.aspx?fileticket=puCa2mOhaFE%3d&tabid=150
Decreto 262 de 2004	28 de enero de 2004	Por el cual se modifica la estructura del Departamento Administrativo Nacional de Estadística DANE y se dictan otras disposiciones	http://www.dane.gov.co/files/acerca/Normatividad/decreto_262.pdf
Documento soporte	Noviembre de 2012	"Régimen de Protección de los Derechos de los Usuarios del Servicio de Televisión y Actualización de la Resolución CRC 3066 de 2011"	http://www.ccit.org.co/files/CRC/DocumentoSoporte_ActualizacionRegimenProteccion_Usuarios_08_11_12.pdf
Sentencia T-729 de 2002	5 de septiembre de 2002	En el presente caso corresponde a la Sala definir si, con la posibilidad de que cualquier persona pueda acceder a datos personales del señor Carlos Antonio Ruiz Gómez, mediante la digitación de su número de identificación, gracias a la manipulación de bases de datos publicadas en sendas páginas de la Internet por parte del Departamento Administrativo de Catastro del Distrito de Bogotá y de la Superintendencia Nacional de Salud, se desconocen sus derechos fundamentales a la autodeterminación informática o a la intimidad.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9903
Documento CONPES 3654 de 2010	12 de abril de 2010	Política de rendición de cuentas de la rama ejecutiva a los ciudadanos	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3654_2010.pdf
Documento CONPES 3650 de 2010	15 de marzo de 2010	Importancia estratégica de la estrategia de gobierno en línea	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3650de2010.pdf
Documento CONPES 3649 de 2010	15 de marzo de 2010	Política Nacional de Servicio al ciudadano	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3649de2010.pdf
Documento CONPES 3292 de 2004	28 de junio de 2004	Proyecto de racionalización y automatización de trámites (Agenda interna)	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3292de2004.pdf

Tipo	Fecha	Objeto	Link
Documento CONPES 3249 de 2003	20 de octubre de 2003	"Política de Contratación Pública para un Estado General".	http://www.mintic.gov.co/index.php/docs-normatividad?pid=698&-sid=764:3249
Documento CONPES 3248 de 2003	20 de octubre de 2003	Renovación de la administración pública	http://programa.gobiernoenlinea.gov.co/normatividad.shtml?scrl=67&apc=b-dx;x;x;x6-&scr_67_G0=7
Documento CONPES 3072 de 2000	9 de febrero de 2000	Agenda de Conectividad	http://programa.gobiernoenlinea.gov.co/normatividad.shtml?scrl=67&apc=b-dx;x;x;x7-&scr_67_G0=8
Directiva presidencial 04 de 2012	3 de abril de 2012	Eficiencia administrativa y lineamientos de la política cero papel en la administración pública	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558a-f042aceeafd1fc4d8/directiva_presidencial_04_de_2012_eficiencia_y_cero_papel.pdf
Directiva Presidencial 10 de 2002	20 de agosto de 2002	Programa de renovación de la administración pública: hacia un Estado comunitario	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558a-f042aceeafd1fc4d8/directiva_10_2002.pdf
Directiva Presidencial 02 de 2000	28 de agosto de 2000	Gobierno en línea	http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558a-f042aceeafd1fc4d8/directiva_02_2000.pdf.

Bibliografía

CAUBIT, R.; BASTOS, A. ISO 27001 e 27002 – Uma visão prática. Editora Zouk, 2009.

DIAS, C. Segurança e auditoria da tecnologia da informação. Axcel Books, 2000.

FONTES, E. Políticas e Normas para a Segurança da Informação. Brasport, 2012.

ICONTEC. Compendio Sistema de Gestión de la Seguridad de la Información (SGSI), segunda ed., 2009.

ICONTEC. Guía para el uso de la norma NTC 5254 Gestión del riesgo dentro del proceso de Auditoría Interna, traducción autorizada al español, realizada por Icontec, 2004.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet. Pearson Education do Brasil, 2003.

LYRA, M. R. Segurança e auditoria em sistema de informação. Ciência Moderna, 2008.

Norma ISO/IEC 18028. Information technology – Security techniques – IT network security, 2005.

Norma ISO/IEC 27005. Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información.

Norma ISO/IEC TR 13335-3. Guidelines for the management of IT security: techniques for the management of IT security, 1998.

Norma NTC ISO/IEC 15999.

Norma NTC ISO/IEC 27001:2006. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos.

Norma NTC ISO/IEC 27002. Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de seguridad de la información. 2 ed., 2005.

PECK, Patrícia. Direito digital: gestão do risco eletrônico. Aspectos legais e éticos do uso da tecnologia. Palestra no evento "Marketing político e Internet", 2006.

SEMOLA, Marcos. Gestão da Segurança da Informação – uma visão executiva. Campus, 2003.

Site Ministerio de las TIC http://www.mintic.gov.co/

Site Presidencia de la República de Colombia http://wsp.presidencia.gov.co/Normativa/Leyes/Paginas/2014.aspx

STALLINGS, W. Network security essentials. Prentice Hall, 2000.

TITTEL, E. Redes de computadores. Colección Schaum. McGraw-Hill, 2004.

Lista de figuras

Lista de tablas

Planeación y Gestión Estratégica de las TI

Versión ESR-Colombia
Escuela Superior de Redes, ESR - Colombia

Se publicó en el mes de julio de 2014,
Publicado por RENATA,
Universidad Nacional de Colombia,
Facultad de Ingeniería
Bogotá D. C., Colombia.
En su diagramación se utilizaron caracteres DaxlinePro

Esta versión está adaptada para Ecuador gracias a CEDIA.

www.cedia.org.ec

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Calle La Condamine 12-109 "Casa Rivera"
Teléfono (+593) 7 405 1000 **Ext.** 4220
info@cedia.org.ec • Cuenca - Ecuador
/FundacionCEDIA @FundacionCEDIA