6. Guías para la Ciberseguridad

2. Principios de Seguridad

2.1 Introducción

La orientación en esta cláusula de la ISO 27032 se centra en tres áreas principales:

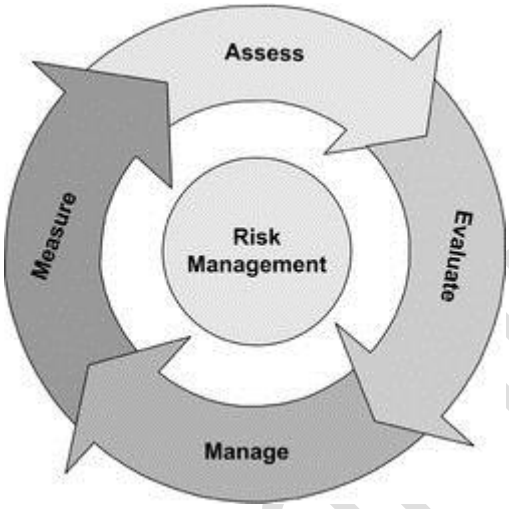
- Una guía de seguridad para los consumidores
- Gestión de riesgos de la seguridad de la información interna de una organización
- Requisitos de seguridad que los proveedores deben especificar para que los consumidores los implementen.

Las recomendaciones se estructuran de la siguiente manera:

a. Una introducción a la **evaluación y gestión de riesgos**
b. Directrices para los **consumidores**
c. Directrices para las **organizaciones**, incluyendo proveedores de servicios:
    a. Gestión de riesgos de la información de seguridad en la empresa
    b. Requisitos de seguridad para los servicios de alojamiento y otros servicios de aplicaciones.

2.2 Evaluación y Gestión de Riesgos

La norma "**ISO 31000**, Gestión de riesgos - Principios y directrices" presenta los principios y guía genéricas sobre la gestión de riesgos, mientras que la norma "**ISO/IEC 27005**, Tecnología de la información - Técnicas de seguridad – Gestión de riesgos de la seguridad de la información" incluye las directrices y los procedimientos para la gestión de riesgos de seguridad de información en una organización, dando soporte, en particular, a los requisitos de un SGSI según ISO/IEC 27001. Estas directrices y procedimientos se consideran suficientes para abordar la gestión de riesgos en el contexto del ciberespacio.



ISO/IEC 27005:2011 no establece ningún método específico para la gestión de riesgos de seguridad de información. Corresponde a los consumidores y proveedores definir su enfoque de gestión de riesgos. Se pueden utilizar una serie de metodologías existentes en el marco descrito en la norma ISO/IEC 27005 para implementar los requisitos de un SGSI.

Un ejemplo es MAGERIT.

Los siguientes aspectos han de tenerse en cuenta al definir el enfoque para la gestión de riesgos:

- **Identificación de activos críticos**: La conexión y el uso del ciberespacio el alcance de la definición de activos. Como no es rentable proteger todos los activos, es esencial que los activos críticos sean identificados de forma que se pueda poner una atención especial para protegerlos. La designación debe hacerse a partir del contexto empresarial, a través de la consideración de los efectos de la pérdida o degradación de un activo de la empresa en su conjunto.
- **Identificación de riesgos**: Los implicados deben considerar y abordar correctamente los nuevos riesgos, amenazas y ataques que se vuelven relevantes cuando participa en el ciberespacio.
- **Responsabilidad**: Al participar en el ciberespacio, un participante debe aceptar la responsabilidad adicional hacia otras partes interesadas. Esto incluye:
    1. **Reconocimiento**: reconocer el posible riesgo que la participación de las partes interesadas podrá introducir en el ciberespacio, en general, y específicamente en los sistemas de información de otras partes interesadas.
        - **Informes**: Puede ser necesario incluir partes interesadas fuera de la organización cuando se distribuyen informes relacionados con los riesgos, incidentes y amenazas.

- **Intercambio de información**: Al igual que con el informe, puede que sea necesario compartir información relevante con otros interesados.
- **Evaluación de riesgos**: Es necesario determinar el grado en que las acciones de un grupo implicados y la presencia en el ciberespacio se convierte en, o contribuye a, un riesgo para la otra parte interesada.
- **Regulador/legislativo**: En la conexión al ciberespacio, los límites legales y regulatorios se vuelven difíciles de distinguir, y a veces son aplicables requisitos contradictorios.

2. **Retirada del sistema o servicio**: Una vez que un sistema o servicio ya no es necesario, debe ser retirado de una manera que asegure que los servicios relacionados o las interfaces no se vean afectadas. Toda la información relacionada con la seguridad debe ser invalidada para asegurar que los sistemas a los que se interconecta o con los que está relacionado no se vean comprometidos.
3. **Consistencia**: El enfoque de la gestión de riesgos se aplica en todo el ciberespacio. Dentro de este enfoque o metodología, los consumidores y los proveedores del ciberespacio se asignan responsabilidades para actividades específicas, tales como la planificación de contingencia, recuperación de desastres y el desarrollo e implementación de programas de protección para los sistemas bajo su control y/o propiedad.

Aspectos importantes a tener en cuenta al considerar las **metas y objetivos de la ciberseguridad** son los siguientes:

- Proteger la seguridad global del ciberespacio
- Planificar emergencias y crisis, mediante la participación en el ejercicio, y la actualización de los planes de respuesta y de continuidad de las operaciones;
- Educar a los interesados en las prácticas de gestión de la ciberseguridad y los riesgos
- Garantizar la compartición de información de forma relevante y precisa entre la policía, los servicios de inteligencia y los tomadores de decisiones clave relacionados con el ciberespacio
- Establecer mecanismos de coordinación eficaces entre sectores y grupos de interés para hacer frente a las interdependencias críticas

2.3 Guías para Consumidores

La norma ISO 27032 no está dirigida a personas individuales del ciberespacio, sino que se centra en las organizaciones que prestan servicios a los consumidores y las organizaciones que requieren que sus empleados o usuarios finales practiquen un uso seguro del ciberespacio para gestionar eficazmente el riesgo de ciberseguridad.

La orientación sobre las funciones y la seguridad de los usuarios en el ciberespacio y cómo podría influir positivamente en el estado de la ciberseguridad tiene como objetivo servir de guía al diseño y desarrollo de contenidos de estas organizaciones, en el contexto de su prestación de servicios, y de programas de sensibilización y formación para su entrega a los usuarios finales.

Como ya hemos comentado, los usuarios pueden ver o recoger información, así como proporcionar cierta información específica dentro del espacio de una aplicación en el ciberespacio, o a un número limitado de miembros dentro del espacio de la aplicación, o al público en general.

Las acciones tomadas por los consumidores en estos roles pueden ser pasivas o activas, y pueden contribuir directa o indirectamente al estado de ciberseguridad.

Por ejemplo, como un IAP (Independent Application Provider), si la aplicación contiene vulnerabilidades de seguridad, podría dar lugar a la explotación que se convertiría en un canal para llegar a los usuarios de la aplicación.

Como bloggers u otras formas de contribuyentes contenidos, pueden recibir una solicitud en forma de preguntas inocentes sobre su contenido en el que involuntariamente pueden revelar más información personal o de la empresa que la deseable.

Como comprador o vendedor, el consumidor, sin saberlo puede participar en operaciones delictivas de venta de bienes robados o actividades de lavado de dinero.

En consecuencia, como en el mundo físico, los consumidores deben tener cuidado con el papel que desempeñan en el ciberespacio.

En general, los consumidores deberían tomar nota de las siguientes recomendaciones:

a. Conocer y comprender la política de seguridad y privacidad del sitio o la aplicación en cuestión, según lo publicado por el proveedor del sitio.
b. Conocer y comprender los riesgos de seguridad y privacidad involucrados y determinar los controles aplicables correspondientes. Participar en foros de discusión en línea relacionados o preguntar a alguien que conozca el sitio o la aplicación antes de proporcionar información personal o de la organización, o antes de participar y aportar información al debate.
c. Establecer y poner en práctica una política de privacidad para proteger la identidad personal mediante la determinación de las categorías de información personal disponible y de los principios relacionados con la distribución de esa información.
d. Gestionar la identidad en línea. Usar identificadores diferentes para aplicaciones web diferentes, y reducir al mínimo el intercambio de información personal para cada sitio web o aplicación que solicite dicha información. Por ejemplo, Single Sign-on es una forma de gestión de identidad.
e. Informar sobre eventos o encuentros sospechosos a las autoridades pertinentes.
f. Como comprador o vendedor, leer y entender las políticas de seguridad y privacidad del mercado en línea, y tomar medidas para verificar la autenticidad de las partes

interesadas involucradas. No compartir información personal, incluida la información bancaria, a menos que se haya confirmado un interés genuino para vender o comprar. Utilizar un mecanismo de pago de confianza.

g. Como IAP, practicar el desarrollo de software seguro y proporcionar un valor hash online del código para que las partes puedan verificar el valor si es necesario para asegurar la integridad del código. Proporcionar documentación de seguridad del código y las políticas y prácticas de privacidad y respetar la privacidad de los usuarios del código.
h. Como blogger o contribuyente de otros contenidos (incluyendo los webmasters), asegurarse de que la privacidad de los interesados y la información sensible no se dan a conocer a través de los blogs o publicaciones en línea. Revisar los comentarios y mensajes recibidos en el sitio y asegurarse de que no contienen ningún contenido malintencionado, como enlaces a sitios web de phishing y descargas maliciosas.
i. Como miembro de una organización, un consumidor individual debe aprender y entender la política corporativa de seguridad de la información de la organización y garantizar que la información clasificada y/o sensible no es liberada intencionalmente o por accidente en cualquier sitio web en el ciberespacio, salvo autorización previa a esta difusión.
j. Otros roles. Cuando un consumidor visita un sitio que requiere autorización y consigue acceder de forma no intencionada, el usuario puede ser etiquetado como un intruso. Salir del sitio de inmediato e informar a la autoridad competente, ya que el hecho de que sea posible conseguir acceso puede ser un indicio de un compromiso.

2.4 Guías para Organizaciones

Los controles para la gestión de riesgos de ciberseguridad dependen en gran medida de la madurez de los procesos de gestión de la seguridad dentro de las organizaciones (incluidos los proveedores de servicios). Si bien las directrices sugeridas aquí son principalmente discrecionales para las organizaciones, se recomienda que los proveedores de servicios traten estas directrices como líneas de base obligatorias.

Las directrices de esta cláusula se puede resumir en:

- Gestionar los riesgos de seguridad de información en la empresa.
- Requisitos de seguridad para alojamiento de webs y otros servicios de aplicaciones.
- **Proporcionar una guía de seguridad para los consumidores**.

A nivel empresarial, las organizaciones que se conectan al ciberespacio deberían implementar un sistema de gestión de seguridad de la información (SGSI) para identificar y gestionar los riesgos relacionados con la seguridad informática para el negocio.

La serie de normas internacionales ISO/IEC 27000 para sistemas de gestión de seguridad de la información proporciona la orientación necesaria y las mejores prácticas para la implementación de dicho sistema.

Como parte de la implementación de un SGSI, una organización también debería establecer un sistema de seguimiento de incidentes de seguridad y la capacidad de respuesta así como la coordinación de sus actividades de respuesta a incidentes con organizaciones externas **CIRT, CERT o CSIRT** en el país.

La provisión de respuesta a incidentes y emergencias debería incluir la vigilancia y la evaluación del estado de seguridad del uso de los servicios de la organización por parte de los usuarios finales y clientes, y proporcionar orientación para ayudar a los afectados en la respuesta a incidentes de seguridad de forma efectiva.

NOTA: La Norma **ISO/IEC 27035**, Tecnología de la información - Técnicas de seguridad - Gestión de Incidentes de Seguridad de la información, proporciona orientación sobre la gestión de incidentes de seguridad de información.

2.4.1 Proporcionar Productos Seguros

Algunas organizaciones desarrollan y lanzan sus propias barras de herramientas para navegador web, dialers, o código para proporcionar valor añadido a los usuarios finales de sus servicios, o para facilitar su acceso a los servicios o aplicaciones de la organización. En tales casos, debe haber un acuerdo de usuario final en un lenguaje adecuado, que incorpore declaraciones sobre la política de codificación y la política de privacidad de la organización, y los medios por los que usuarios pueden cambiar posteriormente su aceptación o escalar cualquier problema que pudieran tener con respecto a la política y las prácticas.

Cuando se usa un acuerdo como este, debe ser colocado bajo el control de versiones y la organización debe asegurarse de que los usuarios finales lo firmen.

Cuando hay un alto grado de dependencia en la seguridad de los productos de software, éstos deben ser validados de forma independiente bajo el esquema Common Criteria, tal como se describe en la norma ISO/IEC 15408.

Las organizaciones deben documentar el comportamiento del código y hacer una evaluación de si el comportamiento puede caer en posibles áreas que pueden ser consideradas como spyware o software engañoso. En este último caso, se debe contratar a un asesor debidamente cualificado para evaluar el código cae dentro de criterios objetivos que usan los proveedores de anti-spyware y que se adhiere a las mejores prácticas para que las herramientas de software proporcionadas por la organización para los usuarios finales, no sean etiquetadas como software espía o adware. Muchos proveedores de anti-spyware publican los criterios por los que clasifican el software.

Las organizaciones deben implementar la firma digital del código para los binarios de forma que los vendedores de anti-malware y anti-spyware puedan fácilmente determinar el propietario de un archivo, así como los ISV (Independent Software Vendor) que producen software que sigue las mejores prácticas, para clasificarlos como seguro incluso antes de hacer el análisis.

Para el cumplimiento de estos requisitos, la formación en seguridad de los desarrolladores es muy importante. Debe utilizarse un ciclo de vida para el desarrollo seguro del software de forma que las vulnerabilidades de software se puedan minimizar proporcionando así un producto de software más seguro.

NOTA: La **Norma ISO/IEC 27034**, Tecnología de la información - Técnicas de seguridad - Seguridad de la Aplicación, proporciona directrices para definir, desarrollar, implementar, administrar, mantener y retirar una aplicación.

2.4.2 Monitorización de Red y Respuesta

La **monitorización de la red** se usa comúnmente en las organizaciones para garantizar la fiabilidad y la calidad de sus servicios de red.

Al mismo tiempo, esta capacidad se puede aprovechar para **buscar condiciones excepcionales** del tráfico de la red y detectar **actividades maliciosas** emergentes.

En general, las organizaciones deben hacer lo siguiente:

- Entender el tráfico en la red - lo que es normal y lo que no es normal.
- Utilizar una herramienta de gestión de red para identificar los picos de tráfico, puertos y tráfico "inusuales" y asegurarse de que hay herramientas disponibles para identificar y responder a la causa.
- Poner a prueba la capacidad de respuesta antes de que se necesite para un evento real. Perfeccionar las técnicas de respuesta, procesos y herramientas basándose en el resultado de los ejercicios regulares.
- Comprender los componentes de forma individual - si alguien que es normalmente un usuario inactivo de repente consume el 100% del ancho de banda disponible, puede ser necesario aislar al usuario hasta que se pueda encontrar la razón. El aislamiento de la red puede prevenir la propagación de malware, aunque algunas implementaciones pueden requerir el consentimiento del usuario o actualizaciones de los Términos de Servicio.
- Considerar la vigilancia de la actividad de puntos de inteligencia de la red, tales como DNS y filtros de mensajería, que también pueden servir para marcar dispositivos que han sido comprometidos con malware pero, por una variedad de razones, no son detectados por los antivirus o servicios de IDS.

2.4.3 Soporte y Escalado

Las empresas, incluidos los proveedores de servicios y las organizaciones gubernamentales suelen tener un servicio de soporte para responder a las consultas de los clientes y proporcionar asistencia técnica y apoyo para hacer frente a los problemas de los usuarios finales.

Con la creciente proliferación de malware a través de Internet, una organización de prestación de servicios puede recibir informes relativos a infecciones de malware y spyware y otros asuntos de ciberseguridad.

Esta información es importante y útil para que los proveedores pertinentes puedan evaluar el riesgo y la situación del malware y proporcionar actualizaciones de las herramientas necesarias para que cualquier nuevo malware o spyware detectado puede ser eliminado o inhabilitado con eficacia.

En este sentido, la organización debe establecer contacto con los proveedores de seguridad y presentar los informes pertinentes y las muestras de software malicioso para que los fabricantes puedan hacer seguimiento - en particular si parece que hay un aumento en la prevalencia. La mayoría de los fabricantes tienen una lista de correo para recibir tales informes o muestras para el análisis y seguimiento.

2.4.4 Mantenerse Actualizados

Como parte de la implementación del SGSI para gestionar el riesgo de la seguridad de la información de la empresa, así como para garantizar que las organizaciones continúan el seguimiento de las mejores prácticas de la industria y se mantienen al día con las últimas vulnerabilidades y exploits, las organizaciones deben participar en la comunidad o en los foros de la industria para compartir sus mejores prácticas y aprender de otros proveedores.

2.4.5 Requisitos para Hosting

La mayoría de los proveedores de servicios ofrecen servicios de alojamiento en sus redes y centros de datos como parte de su negocio. Estos servicios, que incluyen sitios web y otras aplicaciones en línea, a menudo se vuelven a empaquetar y revender por los suscriptores de alojamiento a otros consumidores, tales como pequeñas empresas y usuarios finales. Si los suscriptores de hosting configuran un servidor inseguro, o albergan contenido malicioso en sus sitios o aplicaciones, la seguridad de los consumidores se verá afectada negativamente. Por lo tanto, es importante que los servicios, como mínimo, **apliquen los estándares de mejores prácticas** cumpliendo las políticas o los términos de los acuerdos.

Cuando se utilizan múltiples proveedores, la interacción entre los proveedores debe ser analizada y los acuerdos de servicio respectivos deben tratar con cualquier interacción crítica.

Por ejemplo, las actualizaciones o parches a los sistemas de un proveedor deben coordinarse con otros proveedores, si el resultado de la actualización es una interacción negativa.

Los términos de los acuerdos deben cubrir al menos los siguientes:

a. **Notificaciones claras**, que describan las prácticas de seguridad y privacidad del sitio en línea o de las aplicaciones, las prácticas de recopilación de datos y el comportamiento de cualquier código (por ejemplo, el Browser Helper Object) que el sitio en línea o la

aplicación pueda distribuir y ejecutar en equipos de escritorio de los usuarios finales o en entornos web del navegador.

b. El **consentimiento del usuario**, facilitando el acuerdo o desacuerdo del usuario con los términos de los servicios descritos en las Notificaciones. Esto permitiría a un usuario determinar si puede aceptar los términos de los servicios.
c. **Controles de usuario**, lo que facilita a los usuarios cambiar su configuración o terminar su aceptación en cualquier momento, después del acuerdo inicial.

Los términos deben ser desarrollados con la ayuda de un profesional del derecho para garantizar que también indemnizará al proveedor de servicios ante una posible acción legal de los usuarios finales, como consecuencia de las pérdidas o daños ocasionados debido a contenidos maliciosos o políticas y prácticas poco claras en el sitio web.

Además de la protección de datos personales y las disposiciones de privacidad en el sitio en línea o en las aplicaciones, los proveedores de servicios deben exigir a los sitios o aplicaciones alojadas en sus redes que pongan en práctica un conjunto de mejores prácticas de controles de seguridad a nivel de aplicación antes de que entren en funcionamiento (los veremos en el siguiente módulo).

2.4.6 Guía de Seguridad para Clientes

Los proveedores de servicios deben orientar a los consumidores sobre cómo mantenerse seguros en línea.

Los proveedores de servicios o bien puede crear la guía directamente, o referir a los usuarios a sitios de orientación disponibles que podrían ofrecer los contenidos.

Es fundamental educar a los usuarios finales sobre la forma en que pueden contribuir a una Internet segura en relación con las múltiples funciones que pueden desempeñar en el ciberespacio.

Además, a los usuarios finales se les debe recomendar que apliquen los controles de seguridad técnica necesarios en los que los proveedores de servicios también podrían desempeñar un papel activo.

Entre los ejemplos de actividades de orientación podemos incluir:

a. Boletines de seguridad periódicos (por ejemplo, mensualmente) para asesorar sobre técnicas de seguridad específicas (por ejemplo, cómo elegir una buena contraseña); actualizaciones sobre tendencias de seguridad, y para proveer notificaciones de webcasts de seguridad, otros vídeos bajo demanda, transmisiones de audio e información de seguridad que está disponibles desde el portal web de la organización o de otros proveedores de contenido de seguridad.
b. Emisiones directas de vídeos bajo demanda de formación en seguridad o emisiones por Internet que cubran una variedad de temas de seguridad para mejorar las prácticas de los usuarios finales en seguridad y sensibilización.
c. Seminarios de seguridad o road shows anuales o con otra periodicidad para usuarios finales, posiblemente en colaboración con otras empresas del sector, proveedores y gobiernos

Los proveedores de servicios que utilizan el **correo electrónico** como principal forma de comunicación con los usuarios finales deben hacerlo de una manera que ayude a los usuarios a protegerse de los ataques de ingeniería social. En particular, a los usuarios finales se les debe recordar constantemente que los correos electrónicos no solicitados que lleguen del proveedor de servicio nunca le pedirán:

- Información personal
- Nombres de usuarios
- Contraseñas
- Nunca incluirán enlaces relacionados con la seguridad para que el lector haga clic.

Cuando un proveedor de servicios desee que un usuario visite su sitio para obtener información le indicará **cómo conectar de forma segura**.

Por ejemplo, se puede pedir a un usuario que escriba una URL en el navegador y se asegurará de que la URL citada no contiene un enlace.