7. Controles de Ciberseguridad

1. Contramedidas contra Ataques de Ingeniería Social

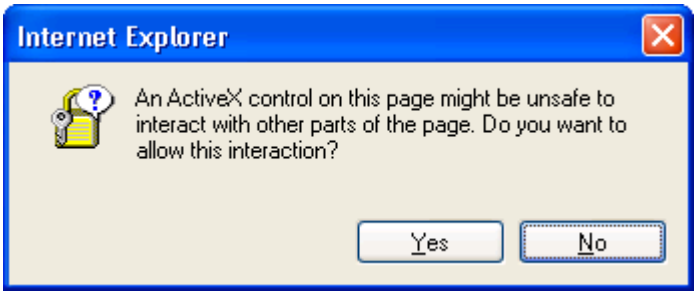
1.1 Introducción

Una vez que se han identificado los riesgos para la ciberseguridad y se han redactado las directrices apropiadas, pueden seleccionarse y aplicarse los controles de seguridad que dan soporte a los requerimientos de seguridad.

Este módulo da una visión general de los controles de ciberseguridad clave que se pueden implementar para apoyar a los lineamientos establecidos en esta norma internacional.

1.2 Controles a Nivel de Aplicación

Entre los controles de nivel de aplicación se incluyen los siguientes:



- **Mostrar avisos breves**, que proporcionen resúmenes claros y concisos, de una página, (usando un lenguaje sencillo) de las políticas online esenciales de la compañía. Estos avisos cortos deben cumplir con todos los requisitos reglamentarios y deben proporcionar enlaces a declaraciones legales completas y otra información pertinente, para que los clientes que deseen más detalles pueden hacer clic para leer la versión más larga.
- **Manejo seguro de las sesiones** para las aplicaciones web, lo que puede incluir mecanismos en línea tales como cookies.
- **Validación de entrada** para prevenir ataques comunes como inyección SQL. Basándonos en el hecho de que los sitios web, que son generalmente considerados como fiables, se utilizan cada vez más para la distribución de código malicioso, la validación de la entrada y la salida tiene que ser llevada a cabo tanto en el contenido activo como en el contenido dinámico.
- **Scripting seguro** de páginas web para prevenir ataques como XSS.
- Probar la El servicio prestado por la organización, ya sea proporcionado por la organización o por un tercero en representación de la organización, deberá entregarse de forma que **el consumidor pueda autenticar el servicio**. Esto puede incluir que el proveedor utilice un subdominio del nombre de dominio de la organización y posiblemente el uso de credenciales HTTPS registrados en la organización. El servicio debe evitar el uso de métodos engañosos donde el consumidor pueda tener dificultades para determinar con quién están tratando y revisarlo por entidades cualificadas.

1.3 Protección del Servidor

Los controles siguientes se pueden utilizar para proteger los servidores de accesos no autorizados y del alojamiento de contenido malicioso en los servidores:

- Configurar los servidores, incluyendo los sistemas operativos subyacentes de acuerdo a una **guía de referencia configuración de seguridad**. Esta guía debe incluir una definición adecuada de los usuarios y administradores del servidor, la aplicación de los controles de acceso a los archivos y directorios de programas y sistema, la habilitación de la auditoría, en particular, para los eventos de fallos de seguridad y de otro tipo en el sistema. Además, se recomienda instalar un sistema mínimo en un servidor con el fin de reducir el vector de ataque.
- Implementar un sistema para **probar e implementar actualizaciones de seguridad**, y asegurar que el sistema operativo del servidor y las aplicaciones se mantienen al día rápidamente cuando haya disponibles nuevas actualizaciones de seguridad.
- Supervisar el **rendimiento de seguridad** del servidor a través de revisiones periódicas de los registros de auditoría.
- Revisar la **configuración de seguridad**.
- Ejecutar **controles antimalware** (tales como antivirus y antispyware) en el servidor.
- Analizar todo el contenido alojado y actualizado periódicamente utilizando **controles de software malicioso actualizados**. Reconocer que un archivo puede ser spyware o malware incluso si no es detectado por los controles actuales, debido a las limitaciones de la información imperfecta.
- Realizar **evaluaciones periódicas de vulnerabilidad** y pruebas de seguridad a los sitios y aplicaciones en línea para asegurarse de que su seguridad está debidamente mantenida.
- Regularmente **buscar compromisos**.

1.4 Controles de Usurario Final

La siguiente es una lista incompleta de los controles que los usuarios finales pueden utilizar para proteger sus sistemas contra ataques conocidos y exploits:

- Uso de **sistemas operativos con soporte** y con los parches de seguridad más actualizados instalados.
- Uso de **aplicaciones de software con soporte** y con los parches más actualizados instalados.
- El uso de **antivirus y herramientas antispyware**. Si es posible, un proveedor de servicios como un ISP debe considerar asociarse con proveedores de seguridad fiables para ofrecer a los usuarios finales estas herramientas como parte del paquete de suscripción de servicio, para que los controles de seguridad estén disponibles a la firma de la suscripción, o al renovar.
- Los consumidores de una organización tienen la responsabilidad de **ser conscientes, y seguir las políticas de la organización sobre el uso de herramientas de software de seguridad**. Los consumidores individuales deben utilizar herramientas de software de seguridad. Se debe consultar al proveedor por cualquier software recomendado. En todos los casos, el software de seguridad debe mantenerse al día con respecto a los parches de seguridad y bases de datos de firmas.
- **Poner en funcionamiento antivirus y antispyware**. Los navegadores y las barras de herramientas de navegador actuales han incorporado capacidades tales como bloqueadores de ventanas emergentes, lo que evitará que sitios web maliciosos muestren ventanas que contienen spyware o software engañoso que permita aprovechar las debilidades del sistema o navegador, o que utilicen la ingeniería social para engañar a los usuarios para descargar e instalarlos en sus sistemas.
- **Las organizaciones deben establecer una política para permitir el uso de dichas herramientas**. Las organizaciones que prestan servicios deben recopilar una lista de herramientas recomendadas, y debe animar a su uso a los usuarios finales, con directrices para su habilitación y concesión de permisos para los sitios web que los usuarios deseen permitir.
- **Habilitar bloqueadores de scripts**. Activar bloqueadores de scripts o ajustes de seguridad web para garantizar que sólo se ejecutan los scripts de fuentes de confianza.

- **Utilizar filtros de phishing**. Los navegadores y las barras de herramientas de navegador a menudo incorporan esta capacidad, lo que podría determinar si un sitio que el usuario está visitando se encuentra dentro de una base de datos de sitios web de phishing conocidos, o contiene patrones de secuencias de comandos que son similares a los encontrados en típicos sitios web de phishing. Las organizaciones deben establecer una política para permitir el uso de dichas herramientas.
- Utilizar otras **características de seguridad disponibles en el navegador**. De vez en cuando, cuando surge un nuevo riesgo de ciberseguridad, los navegadores web y los proveedores de barras de herramientas del navegador añaden nuevas capacidades para proteger a los usuarios. Los usuarios finales deben estar al tanto de estos avances. Las organizaciones y proveedores de servicios también deberían revisar estas nuevas capacidades y actualizar las políticas y servicios.
- **Habilitar un firewall personal y un HIDS**. Los sistemas operativos más recientes tienen firewalls personales y HIDS incorporados que están habilitados de forma predeterminada, pero los usuarios o algunas aplicaciones pueden desactivarlos. Las organizaciones deben adoptar una política sobre el uso del firewall personal y el HIDS y evaluar las herramientas adecuadas, de manera que su uso esté habilitado de forma predeterminada para todos los empleados.
- **Activar actualizaciones automáticas**. Los controles anteriores de técnicas de seguridad son capaces de hacer frente a software malicioso en sus niveles respectivos de funcionamiento, pero no son muy eficaces contra la explotación de las vulnerabilidades existentes en los sistemas operativos y aplicaciones.

1.5 Controles contra Ataques de Ingeniería Social

Los cibercriminales están recurriendo cada vez más a tácticas de ingeniería psicológica o social.

Algunos ejemplos:

- Correos electrónicos que llevan URI para dirigir a los usuarios incautos a sitios web de phishing.
- Correos de estafa que solicitan a los usuarios información de identificación personal, o información relativa a la propiedad intelectual de las empresas.

La proliferación de redes sociales y sitios de comunidad ofrecen vehículos nuevos que permiten estafas y fraudes más creíbles. Cada vez más, estos ataques también están trascendiendo la tecnología, más allá de los sistemas de PC y conectividad de red tradicional, aprovechando los **teléfonos móviles, redes inalámbricas** (incluyendo Bluetooth) y **voz sobre IP** (VoIP).

La orientación proporcionada en esta cláusula se basa en la idea de que la única forma efectiva para mitigar la amenaza de la ingeniería social es a través de la combinación de:

- Tecnologías de seguridad
- Políticas de seguridad que establezcan normas básicas de comportamiento personal, tanto como individuo y como empleado
- Educación y formación adecuadas.

El marco abarca por lo tanto:

- Políticas
- Métodos y procesos
- Personas y las organizaciones
- Controles técnicos aplicables.

1.5.1 Políticas

En consonancia con las prácticas comunes para la gestión de riesgos de seguridad de información, las **políticas básicas que rigen el uso, creación, recolección, almacenamiento, transporte, distribución, y procesamiento de información de la organización y personal y de la propiedad intelectual en Internet y en el ciberespacio debe determinarse y documentarse**. En particular, esto se refiere a aplicaciones como mensajería instantánea, blogs, intercambio de archivos P2P, y redes sociales, que están normalmente más allá del alcance de la red de la empresa y la seguridad de la información.

Como parte de las políticas corporativas, deben incorporarse las **declaraciones y sanciones relacionadas con el mal uso de las aplicaciones del ciberespacio** para disuadir contra el mal uso por parte de los empleados y terceros en la red corporativa o de los sistemas que acceden al ciberespacio.

Deben elaborarse políticas administrativas que **promuevan la concienciación y la comprensión de los riesgos de ciberseguridad**, y fomenten, o incluso **obliguen**, el aprendizaje y desarrollo de habilidades en contra de los ataques de ciberseguridad, en particular contra los ataques de ingeniería social.

Esto debe incluir requisitos de asistencia regular a reuniones informativas y de capacitación.

1.5.2 Métodos y Procesos

1.5.2.1 Categorización y clasificación de información

Para cada categoría y clasificación de información, deben **desarrollarse y documentarse controles específicos** de seguridad para la protección contra la exposición accidental y el acceso no autorizado.

Deben desarrollarse y publicarse **procedimientos sobre cómo manejar las propiedades intelectuales** de la compañía, datos personales y otra información confidencial.

1.5.2.2 Concienciación y formación

Como parte del programa de ciberseguridad de la organización, **los empleados y contratistas deben ser obligados a someterse a un número mínimo de horas de formación de sensibilización** con el fin de asegurarse de que son conscientes de sus roles y responsabilidades en el ciberespacio, y de los controles técnicos que deberían implementar como personas que utilizan el ciberespacio.

Además, como parte del programa para contrarrestar los ataques de ingeniería social, la formación de sensibilización debería incluir contenidos tales como los siguientes:

- Las amenazas y formas de ataque de ingeniería social más recientes, por ejemplo, cómo ha evolucionado el **phishing** de sitios web falsos a una combinación de spam, Cross Site Scripting, y ataques de inyección SQL.
- Cómo la **información individual y corporativa puede ser robada y manipulada** a través de ataques de ingeniería social, explicando cómo los atacantes pueden aprovechar la naturaleza humana, como la **tendencia a cumplir las peticiones que se hacen por parte de**

una autoridad, amabilidad, hacerse pasar por una víctima, o la reciprocidad, en primer lugar dar algo de valor o ayuda.

- **Qué información debe protegerse** y la forma de hacerlo, de conformidad con la política de seguridad de la información.
- **Cuándo informar o escalar un evento sospechoso** o una aplicación maliciosa a las autoridades, así como información sobre estos contactos disponibles.

Las organizaciones que ofrecen aplicaciones en el Ciberespacio y servicios en línea **deben proporcionar materiales de sensibilización a los suscriptores o usuarios** que cubran los contenidos anteriores dentro del contexto de sus aplicaciones o servicios.

1.5.2.3 Pruebas

Los empleados deben firmar un acuerdo en el que aceptan y comprenden el contenido de la política de seguridad de la organización.

Como parte del proceso para mejorar el conocimiento y asegurar la debida atención a estos riesgos, una organización debería considerar la realización de pruebas periódicas para determinar el nivel de conocimiento y cumplimiento de las políticas y prácticas relacionadas.

Los empleados pueden realizar **una prueba escrita o someterse a CBT** (Computer Based Training) para determinar si entienden el contenido de la política de seguridad de la organización.

Estas pruebas pueden incluir, aunque no se limitan a la creación de sitios específicos y controlados de phishing, y correos fraudulentos que utilicen contenidos creíbles de ingeniería social.

Al llevar a cabo estas pruebas, es importante asegurarse de que:

- Los servidores de prueba y los contenidos se encuentran **bajo el control** del equipo de pruebas
- Los profesionales que tienen experiencia previa en dicha prueba **se implican** siempre que sea posible
- **Los usuarios están preparados** para estas pruebas a través de los programas de sensibilización y formación
- Todos los resultados de las pruebas **se presentan en forma agregada** con el fin de proteger la privacidad de un individuo.

1.5.3 Personas y Organización

Mientras que los individuos son los principales objetivos de los ataques de ingeniería social, una organización también puede ser la víctima. Las personas, sin embargo, siguen siendo el principal punto de entrada para los ataques de ingeniería social. Por lo tanto, **las personas deben ser conscientes de los riesgos relacionados con el ciberespacio y las organizaciones deben establecer políticas pertinentes y adoptar medidas proactivas para patrocinar programas relacionados que aseguren la concienciación y capacitación de las personas**.

Como regla general, todas las organizaciones (incluyendo empresas, proveedores de servicios, y gobiernos) **deben alentar a los consumidores en el ciberespacio a aprender y entender los riesgos de ingeniería social**, y los pasos que deben tomar para protegerse contra posibles ataques.

1.5.4 Técnica

Además de establecer las políticas y prácticas contra los ataques de ingeniería social, **los controles técnicos también deben tenerse en cuenta** y de ser posible, ser adoptados para minimizar la exposición.

En el módulo anterior ya hemos presentado guías para personas y organizaciones que pueden aplicarse.

Además, deben considerarse los siguientes controles técnicos que son útiles contra ciertos ataques de ingeniería social:

- Dónde esté implicada información personal o confidencial corporativa en las aplicaciones en línea, deben considerarse **soluciones de autenticación fuerte** ya sea como parte de la autenticación de inicio de sesión, y/o cuando las operaciones críticas se están ejecutando. La autenticación fuerte se refiere a la utilización de dos o más factores adicionales de verificación de identidad, más allá de la utilización de un ID de usuario y contraseña. El segundo factor y los adicionales se pueden proporcionar mediante tarjetas inteligentes, biometría, u otros tokens manuales de seguridad.
- Para los servicios basados en web, las organizaciones deben considerar el uso de un "**High Assurance Certificate**" para proporcionar seguridad adicional a los usuarios en línea. La mayoría de las Autoridades Certificadoras (CA) comerciales y los navegadores web son capaces de soportar el uso de dichos certificados, los cuales reducen la amenaza de ataques de phishing.
- Para garantizar la seguridad de los ordenadores de los usuarios que se conectan a la organización o al sitio del proveedor de servicio o a una aplicación en el ciberespacio, deben considerarse controles adicionales para asegurar un nivel mínimo de seguridad, como la instalación de las actualizaciones de seguridad más recientes. El uso de controles debe publicarse en el contrato de servicios para el usuario final y/o en la Política de Privacidad del Sitio.

1.6 Otros Controles

Otros controles técnicos aplicables son:

- **Darknet Monitoring**
- **Backscatter**
- Investigación mediante **Traceback**
- Respuestas mediante **Sinkhole Operation**
- Correlación de eventos del proveedor de eventos y elementos empresariales como servidores DNS, flujo de red de routers, filtrados de mensajes de salida y comunicaciones P2P.
- Cuarentena de dispositivos.