6. Guías para la Ciberseguridad

1. Guías para usuarios

1.1 Introducción

Para mejorar el estado de ciberseguridad, los implicados en el ciberespacio tienen que jugar un papel activo en su respectivo uso y en el desarrollo de Internet.

Estos papeles pueden a veces superponerse con sus roles individuales y organizativos dentro de sus redes personales o de la organización.

El término red de la organización se refiere a la combinación de redes privadas de una organización (típicamente una intranet), extranets y redes públicamente visibles.

A los efectos de norma ISO 27032, las redes públicamente visibles son las redes expuestas a Internet, por ejemplo para alojar un sitio web.

Empezaremos viendo cuáles son los roles que juegan los diferentes interesados en la ciberseguridad.

1.2 Roles en Ciberseguridad

1.2.1 Consumidores

Los consumidores pueden ver o recoger información, así como proporcionar cierta información específica dentro del espacio de una aplicación en el ciberespacio, o de forma limitada a los miembros o grupos dentro del espacio de la aplicación, o el 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 seguridad cibernética.

Los consumidores individuales del ciberespacio pueden asumir diferentes roles en diferentes contextos y aplicaciones:

- Usuario de una aplicación del ciberespacio o usuario general, como un jugador de juego en línea, usuario de mensajería instantánea, o internauta
- Comprador/vendedor que participan en la colocación de productos y servicios en línea y sitios de subasta para los compradores interesados, y viceversa
- Blogger o colaborador de otro contenido (por ejemplo, un autor de un artículo en una wiki), donde la información se publica en forma de texto o multimedia (por ejemplo, clips de video) para el consumo público o para una audiencia limitada
- IAP dentro de un contexto de aplicación (por ejemplo, un juego en línea), o el ciberespacio en general
- Miembro de una organización (por ejemplo, un empleado de una compañía, u otra forma de asociación con una empresa)
- Otros roles. Es posible que a un usuario se le pueda asignar un rol sin querer o sin su consentimiento. Por ejemplo, cuando un usuario visita un sitio que requiere autenticación, pero consigue acceso de forma no intencionada, el usuario puede ser etiquetado como intruso

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

- **Ejemplo**: Si un IAP ofrece una aplicación que contiene vulnerabilidades de seguridad, estas vulnerabilidades pueden ser utilizadas por malhechores como un canal para llegar a los usuarios de la aplicación.

- **Ejemplo**: Bloggers u otras formas de generadores de contenido pueden recibir una solicitud en forma de preguntas inocentes sobre su contenido. En su respuesta, sin querer, pueden revelar más información personal o de la empresa de lo deseable.
- **Ejemplo**: Un individuo, actuando como comprador o vendedor, sin saberlo, pueden participar en operaciones delictivas de la venta de bienes robados o actividades de lavado de dinero.

En consecuencia, como en el mundo real, los consumidores individuales deben tener precaución en todos y cada uno de los papeles que desempeñan en el ciberespacio.

Por otra parte, las organizaciones a menudo utilizan el ciberespacio para dar a conocer la empresa e información relacionada, así como para la comercialización de productos y servicios.

Las organizaciones también utilizan el ciberespacio como parte de su red para la entrega y recepción de mensajes electrónicos (por ejemplo, correo electrónico) y otros documentos (por ejemplo, transferencia de archivos,).

De acuerdo con los mismos principios de ser un buen ciudadano corporativo, estas organizaciones deberían extender sus responsabilidades corporativas al ciberespacio de forma proactiva para asegurar que sus prácticas y acciones en el ciberespacio no introducen nuevos riesgos de seguridad.

Algunas medidas preventivas son:

- Gestión adecuada de la seguridad de la información mediante la implementación y operación eficaz de un sistema de gestión de la seguridad de la información (SGSI). ISO 27001 proporciona los requisitos para un SGSI.
- Adecuada monitorización de la seguridad.
- La incorporación de la seguridad como parte del ciclo de vida del desarrollo de software (SDLC), donde el nivel de seguridad integrada en los sistemas tiene que ser determinado con base en la criticidad para la organización de los datos
- Educación en seguridad de los usuarios en la organización a través de actualizaciones tecnológicas continuas y el seguimiento de los desarrollos de última tecnología
- Comprender y utilizar los canales adecuados de comunicación con proveedores y prestadores de servicios en materia problemas de seguridad descubiertos durante el uso.

Como soporte a esta norma:

- El estándar ISO/IEC 29147 proporcionará guías para la revelación de vulnerabilidades
- ISO/IEC 27031 proporciona guías para la preparación de la continuidad de negocio en ICT
- ISO/IEC 27035 proporciona guías para la gestión de incidentes de seguridad de la información
- ISO/IEC 27034-1 proporciona guías para la seguridad en aplicaciones

El gobierno y, principalmente las fuerzas de seguridad y los organismos reguladores, pueden tener los siguientes roles importantes que desempeñar:

- Asesorar a las organizaciones de sus roles y responsabilidades en el ciberespacio
- Compartir información con otras partes interesadas sobre las últimas tendencias y desarrollos en la tecnología;

- Compartir información con otras partes interesadas sobre los riesgos de seguridad actuales
- Ser un conducto para recibir cualquier información, ya sea cerrado o abierto, con respecto a los riesgos de seguridad en el ciberespacio
- Ser el coordinador principal para la difusión de información y la orquestación de todos los recursos necesarios, tanto a nivel nacional como a nivel corporativo, en tiempos de crisis resultantes de un ataque masivo.

1.2.2 Proveedores

Las organizaciones que proveen servicios las podemos dividir en dos categorías:

- Proveedores de acceso a empleados y socios en el ciberespacio
- Proveedores de servicios a los consumidores del ciberespacio, ya sea para una comunidad cerrada (por ejemplo, los usuarios registrados), o el público en general, a través de la entrega de aplicaciones en el ciberespacio

Algunos ejemplos de servicios son los marketplaces de trading, el comercio en línea, los servicios de foros de discusión, los servicios de plataforma de blogs, y los servicios de redes sociales.

Los proveedores de servicios son también organizaciones consumidoras y por lo tanto deben observar las mismas funciones y responsabilidades que estas.

Como proveedores de servicios, tienen responsabilidades adicionales para mantener o mejorar incluso la seguridad del ciberespacio:

- Suministrar productos y servicios seguros y protegidos
- Proporcionar seguridad y directrices de seguridad para los usuarios finales,
- Proporcionar información de seguridad a otros proveedores y a los consumidores acerca de las tendencias y observaciones de tráfico en sus redes y servicios.