EL NUEVO ECUADOR

Ministerio del Interior
Ministerio de Turismo

GUÍA DE BUENAS PRÁCTICAS PARA LA PREVENCIÓN DE LA CIBERDELINCUENCIA EN ESTABLECIMIENTOS TURÍSTICOS.

DIRECCIÓN DE CIBERDELITOS

FEBRERO 2025

Guía de buenas prácticas para la prevención de la Ciberdelincuencia en Establecimientos Turísticos.

Ministerio del Interior

Viceministerio de Seguridad Pública

Subsecretaría de Combate al Delito

Dirección de Ciberdelitos

Presidente de la República
MAGISTER DANIEL NOBOA AZÍN

Ministro del Interior
GRAD. (S.P.) FAUSTO BUENAÑO CASTILLO

Viceministro de Seguridad Pública (E)
DOCTOR LYONEL CALDERON TELLO

Subsecretario de Combate al Delito
TCNL. (S.P.) LUIS PÉREZ DÁVILA

Director de Ciberdelitos
MAGISTER FERNANDO ILLESCAS PEÑA

Responsables y Colaboradores
Redacción técnica del documento:
INGENIERO DIEGO TEJADA CAMPOS, Analista de Ciberdelitos
MAGISTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos

Redacción legal:
MAGISTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos

Revisión y Adaptación:
MAGISTER JORGE NEJER GUERRERO, Especialista de Ciberdelitos
MAGISTER FERNANDO MOYA LEIMBERG, Especialista de Ciberdelitos
INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

Versión 1.1

Tabla de contenido

Introducción

La creciente digitalización ha transformado la forma de hacer negocios en el mundo, impulsando la creación de servicios accesibles y personalizados (Mentsiev, Engel, & Tsamaev, 2020). En el sector turístico, las plataformas y herramientas tecnológicas, permiten a los establecimientos optimizar procesos como reservas, pago de bienes o servicios en línea, entre otros, mejorando así la experiencia de los usuarios. No obstante, esta digitalización genera paralelamente riesgos que afectan tanto a los negocios como a sus usuarios.

Estos riesgos incluyen actividades sospechosas o ilícitas que van desde fraudes electrónicos y robo de datos personales, hasta el aprovechamiento de plataformas tecnológicas o aplicaciones que facilitan el cometimiento de otro tipo de delitos que atentan contra la integridad y derechos de las personas. Las empresas turísticas, debido a la constante actividad de internautas, generan un alto volumen de transacciones y consecuentemente el almacenamiento de información sensible, esto hace que sean atractivas para la delincuencia común y la ciberdelincuencia.

Hasta enero del año 2025, en el Ecuador se encuentran registrados por el Ministerio de Turismo (MINTUR) 5.321 establecimientos de alojamiento y 19.996 servicios de alimentos y bebidas: https://servicios.turismo.gob.ec/catastro-turistico/ tales como hoteles, hostales, restaurantes, bares, discotecas, entre otros. Cabe indicar que existe una alta presencia de establecimientos informales, que están fuera del control regulatorio, lo que incrementa el riesgo de ser afectados por la ciberdelincuencia.

A nivel global, la percepción de la seguridad digital se enfoca principalmente en la protección de sistemas tecnológicos, dejando en segundo plano el factor humano. El informe "IBM X-Force Threat Intelligence Index 2024" indica que el 30% de los incidentes analizados, se debieron al acceso mediante cuentas legítimas vulneradas a través de enlaces de phishing, contraseñas débiles, descuido en la supervisión de accesos, entre otros, que evidencian la necesidad de trabajar con el usuario final en temas de seguridad digital (IBM Security, 2024).

La ausencia de cultura y responsabilidad digital es aprovechada por los ciberdelincuentes, situación que se maximiza con los avances de la inteligencia artificial, la cual actualmente puede ser utilizada entre otras aplicaciones para generar comunicaciones falsas o simular conversaciones telefónicas; este tipo de ataques no compromete sistemas, sino que vulnera directamente la integridad de las personas. Por ello, es fundamental que tanto los usuarios de servicios como los establecimientos de servicios turísticos, conozcan acerca de buenas prácticas para prevenir estos riesgos.

En este contexto, el Ministerio del Interior a petición del Ministerio de Turismo, ha desarrollado la ***"Guía de buenas prácticas para la prevención de la Ciberdelincuencia en Establecimientos Turísticos"***, cuyo propósito es establecer medidas preventivas aplicables a toda actividad inherente a los servicios turísticos. Esta guía ofrece una serie de recomendaciones prácticas que ayudan a los prestadores de servicios turísticos a adoptar medidas de prevención, asegurar de redes de datos y proteger los datos personales, minimizando así el cometimiento de delitos.

Objetivo

Proporcionar recomendaciones prácticas y controles generales para los establecimientos turísticos y sus usuarios, con el fin de prevenir el cometimiento de delitos mediante el uso de tecnologías digitales, promoviendo un entorno digital seguro y protegido para todos los actores de este sector.

Ámbito de aplicación y alcance

La presente guía ofrece recomendaciones prácticas dirigidas a los establecimientos turísticos para prevenir el cometimiento de delitos utilizando tecnologías digitales. Las medidas están diseñadas para propietarios de negocios, empleados y usuarios de servicios turísticos, enfocándose en acciones preventivas, protección de datos personales, transacciones electrónicas y redes de datos, entre otros que ayuden a prevenir y combatir los posibles delitos.

Es importante señalar que la aplicación de esta Guía no sustituye políticas internas de seguridad digital ni la responsabilidad de cumplimiento de la normativa legal vigente.

Base Legal

Tabla 1 - Artículos de la Normativa Legal Vigente

Cuerpo normativo	Artículos
Constitución de la República del Ecuador	3, 6, 10, 15, 16, 17, 30, 31, 66, 75, 76, 83, 85, 194, 195, 226, 335, 336, 337, 341, 385, 393.
Código Orgánico Integral Penal	11, 18, 22, 23, 25, 29, 34, 409, 410, 411, 421, 423, 427, 428, 429, 430, 441, 442, 443, 444, 453, 458.
Ley Orgánica de Protección de Datos Personales	1, 2, 3, 7, 8, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 33, 34, 35, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48, 49, 50, 52, 75, 76.
Ley de Turismo	2, 3, 4, 5, 43, 44, 45, 46, 48, 49, 50, 51. Capítulo (...) De las Modalidades De Turismo (Capítulo agregado por el Art. 9 Cap. I de la Ley s/n, R.O. 525-S, 25-III-2024) Art. (...). Capítulo (...) Del Turismo Comunitario (Capítulo agregado por el Art. 9 Cap. I de la Ley s/n, R.O. 525-S, 25-III-2024) Art. (...).
Reglamento a la Ley Orgánica de Protección de Datos Personales	Articulado íntegro
Resolución Nro. JPRM-2024-018-M de la Junta de Política y regulación monetaria	Disposición General Quinta

I

USUARIOS DE SERVICIOS TURÍSTICOS

EL NUEVO ECUADOR

Ministerio del Interior

GUÍA DE BUENAS PRÁCTICAS PARA LA PREVENCIÓN DE LA CIBERDELINCUENCIA EN ESTABLECIMIENTOS TURÍSTICOS.

Buenas Prácticas para Usuarios de Servicios Turísticos

Cuando se organizan y realizan actividades turísticas, la atención se dispersa entre múltiples responsabilidades, como logística del viaje, itinerarios, llamadas del trabajo, cuidado de los hijos, mascotas, entre otros; esto incrementa la exposición y la vulnerabilidad, lo que puede ser aprovechado por quienes buscan perpetrar delitos en entornos digitales de carácter turístico. Por ello, es esencial anticipar posibles vulnerabilidades del entorno de los usuarios de servicios turísticos y utilizar las tecnologías digitales de manera consciente, atenta y responsable, garantizando así una experiencia segura y placentera en los servicios turísticos.

1. Verificación de establecimientos formales

Para favorecer una experiencia confiable y segura al contratar servicios turísticos que se promocionan a través de internet, es importante optar por establecimientos de turismo genuinos, ya sean agencias de viaje, hoteles, restaurantes, aerolíneas, bares, entre otros, los cuales deben estar debidamente registrados en el Ministerio de Turismo. De esta manera, se garantiza que el servicio ofrecido sea formal. La validez del registro de estos establecimientos puede ser verificada en el siguiente enlace:

https://servicios.turismo.gob.ec/catastro-turistico/

2. Uso seguro de redes Wi-Fi

Las redes Wi-Fi son una herramienta útil en espacios turísticos, por lo que es importante tomar precauciones para proteger la información personal y prevenir delitos que son cometidos mediante el uso de tecnologías digitales, por lo que, en la medida de lo posible, se debe evitar la conexión a redes Wi-Fi libres (Kemp, 2023). A continuación, se presentan las siguientes recomendaciones:

Verificar la autenticidad de la red: Confirmar siempre el nombre de la red oficial del establecimiento antes de conectarse, evitando ingresar a redes falsas; el establecimiento deberá contar con una política de seguridad dirigida a los usuarios de servicios turísticos donde se detalle el uso de la o las redes wifi del establecimiento.

Utilizar datos móviles para transacciones importantes: Para transacciones bancarias o compras en línea, es preferible utilizar sus propios datos móviles contratados con su operadora celular, o a su vez consultar la política de seguridad digital del establecimiento, el cual deberá garantizar la seguridad de sus redes.

Utilizar sitios seguros: Al navegar en internet, especialmente a sitios web de bancos o al realizar compras en línea que contemplen pagos con tarjetas de crédito o transacciones, asegurarse de ingresar al sitio web oficial y que el mismo tenga la seguridad HTTPS **(** 🔒 **)** en la barra del navegador y, en la medida de lo posible, activar notificaciones bancarias para detectar transacciones no autorizadas.

Crear contraseñas robustas en dispositivos personales: Para el acceso a sus dispositivos y aplicaciones, es necesario utilizar contraseñas seguras con un mínimo de 8 caracteres y una combinación de letras, números y símbolos considerando que en la actualidad existen muchos mecanismos para vulnerar contraseñas simples. Si el dispositivo cuenta con un sensor biométrico, es recomendable configurar la autenticación biométrica de huella digital o reconocimiento facial.

Autenticación multifactorial (MFA) en tus servicios en línea: Activar MFA agrega una capa extra de protección en cuentas personales, debido a que el ingreso requerirá otra verificación, como un código enviado al correo electrónico del usuario, lo que dificulta el acceso a terceros, incluso si logran obtener la contraseña principal. Este método es conocido como doble factor de autenticación (Ruslan, 2024).

Utilizar antivirus confiables: Es recomendable contar con un software antivirus instalado en dispositivos como computadores, tabletas, celulares, entre otros. En lo posible, se debe optar por antivirus comerciales con trayectoria comprobada.

Mantener actualizados los dispositivos: Las actualizaciones de Windows, Android, iOS o el firmware de los dispositivos, así como las actualizaciones del software instalado en los dispositivos como los antivirus, corrigen vulnerabilidades de seguridad. Se debe considerar que cada día aparecen nuevas amenazas, por lo que mantener los dispositivos actualizados es fundamental.

Mantener todos los dispositivos con contraseña: Asegurarse que todos los dispositivos tengan contraseña para evitar accesos no consentidos. Es recomendable configurar el bloqueo automático cuando el dispositivo no se encuentre en uso.

Desconectar el Wi-Fi cuando no se use: En la medida de lo posible, se recomienda desactivar la conexión Wi-Fi del dispositivo cuando este no esté en uso. Esto evita que el dispositivo permanezca conectado a la red y quede expuesto innecesariamente.

Cerrar todas las sesiones: Cuando use equipos o dispositivos que no sean personales, como los equipos del hotel, use la navegación en modo incógnito. Al finalizar es importante cerrar todas las cuentas y borrar el historial de navegación del dispositivo y/o documentos generados durante el uso.

Evitar compartir información personal o financiera: Nunca se deben compartir números de tarjetas, contraseñas o documentos por medios electrónicos. Tampoco se debe permitir fotografiar o fotocopiar estos documentos, asegurando el derecho de los usuarios conforme a la normativa legal vigente.

Configurar alertas de instituciones financieras: Se recomienda comunicarse con la entidad financiera y configurar la recepción de alertas de transacciones en tiempo real para detectar movimientos inusuales o no reconocidos. En caso de identificar transacciones sospechosas o no realizadas por el usuario, se debe contactar de inmediato con la entidad y si es posible con el establecimiento que generó la transacción a fin de reportar dichos movimientos.

Evitar abrir aplicaciones innecesarias en redes públicas: En situaciones de estricta necesidad o emergencia podría ser inevitable el uso de estas redes. Para seguridad de navegación, se recomienda instalar y configurar una VPN en los dispositivos.

Mantener software original: Es importante comprender que el software original de los dispositivos permite acceder a actualizaciones y soporte técnico de la marca. Las versiones no oficiales o comúnmente denominadas ´crackeadas´ pueden introducir software malicioso que comprometa datos críticos.

3. Medidas de protección para niñas, niños y adolescentes

Existen ocasiones en las que los usuarios de los servicios turísticos acuden acompañados de niñas, niños o adolescentes, para estos casos se deberá cumplir con lo que establecen las normas y/o reglamentos, para lo cual se deberá llevar un registro de huéspedes, diferenciando entre adultos con menores de edad. Esto permitirá proteger la integridad de niñas, niños y adolescentes y prevenir el cometimiento de delitos en su contra.

Así mismo, el establecimiento de alojamiento debe promover protocolos de seguridad digital para la protección de menores y buenas prácticas de uso de las redes o equipos tecnológicos que se encuentren a disposición del usuario.

Se recomienda a los usuarios configurar la seguridad de sus dispositivos personales y, en caso de utilizar equipos del establecimiento, verificar sus medidas de protección. En todos los casos, es fundamental que los menores cuenten con una supervisión adecuada (Juca-Maldonado & Medina-Peña, 2023).

Supervisión a niñas, niños y adolescentes.

Instruir a las **niñas, niños y adolescentes** para evitar encuentros con desconocidos a través de citas generadas vía internet. Los padres o tutores deben fomentar espacios de comunicación y socialización de los riesgos que presenta el ciberespacio, a fin de prevenir ilícitos como el grooming, el sexting u otras actividades delictivas, manteniendo una supervisión adecuada antes, durante y después de la experiencia turística. (Parder, Gryffroy, & Juurik, 2024)

No compartir información personal y/o sensible con personas desconocidas.

- Si alguien solicita datos personales a las **niñas, niños y adolescentes,** se les debe enseñar a no proporcionarlos, eludir y reportar la conversación o el contacto.
- **Consejo práctico**: Enseña a responder: "pregunta a mi mamá o papá".

Desconectar a los menores del Wi-Fi cuando no lo necesiten.

- Cuando las **niñas, niños y adolescentes** estén descansando o desarrollando actividades que no involucren la tecnología, es recomendable desconectarlos del Wi-Fi, evitando riesgos asociados.
- **Consejo práctico**: Fomentar el hábito de la "hora de desconexión" antes de dormir, a la hora de comer, etc.

Desactivar el Bluetooth y el AirDrop en lugares públicos

- Estos pueden conectarse con otros dispositivos cercanos. Enseña a activarlos solo cuando sea necesario manteniendo la seguridad en los dispositivos.
- **Consejo práctico**: Configurar los dispositivos de modo que la red Bluetooth y el punto de acceso a internet no estén disponibles ni visibles de manera permanente.

Cambiar el nombre de sus dispositivos

- Utilizar un nombre genérico o divertido para los dispositivos, por ejemplo, "Tableta Espía" en lugar de su nombre real. De esta manera, si otros dispositivos los detectan, no revelarán datos personales de a quién pertenecen.

Evitar transmisiones en vivo (streaming) mientras están de viaje

- Si las **niñas, niños y adolescentes** tienen el hábito de realizar transmisiones en vivo o subir videos a plataformas digitales, es importante explicar que es más seguro revisar el entorno previo a hacerlo, evitando compartir información sensible o personal en tiempo real, como ubicación geográfica, nombre del alojamiento, placas del vehículo, documentos personales, entre otros.

- Enseñar a las **niñas, niños y adolescentes** a cuidar de su información personal y evitar que la misma se publique en las diversas plataformas digitales.
- **Consejo práctico**: Enseñar a disfrutar el momento y que las redes sociales pueden quedar para después.

Instalar y configurar controles parentales en dispositivos personales de menores:

- Es recomendable instalar y configurar aplicaciones de control parental. Muchos dispositivos no incluyen esta aplicación; sin embargo, existen diversas herramientas gratuitas que pueden ser instaladas.

II

PRESTADORES DE SERVICIOS TURÍSTICOS

Dirección: Av. Amazonas N24-196 y Luis Cordero, edificio Contempo.
Código postal: 170524 / Quito-Ecuador
www.ministeriodelinterior.gob.ec

Buenas Prácticas para Prestadores de Servicios Turísticos

Los ciberdelincuentes consideran a los establecimientos turísticos una oportunidad para cometer delitos, aprovechando el flujo constante de visitantes, el acceso a redes públicas y la facilidad de operar cerca de sus víctimas sin levantar sospechas; incluso en ciertos casos, utilizan estos lugares para perpetrar delitos relacionados con niños, niñas y adolescentes. Los establecimientos turísticos brindan un entorno temporal y anónimo, donde la atención se centra en otras actividades tanto de los turistas como del personal del establecimiento. Esto favorece el accionar de los ciberdelincuentes, por lo que se resalta la necesidad de implementar medidas de seguridad digital, que protejan tanto a los usuarios de servicios turísticos como la reputación y continuidad del negocio (Kemp, 2023).

Para generar un entorno seguro y reducir los riesgos asociados a la ciberdelincuencia, los empleados pueden aplicar medidas preventivas que se detallan a continuación:

1. Medidas de Protección para Reducir Riesgos

Manejo de Contraseñas

- **Contraseñas Seguras**: Utilizar contraseñas que combinen letras, números y símbolos con un mínimo de 8 caracteres. Cambiarlas regularmente para asegurar la protección de los sistemas. Esto incluye las contraseñas utilizadas para las redes Wi-Fi del hotel, sistemas de reservas, portales bancarios, cuentas del Servicio de Rentas Internas (SRI), Instituto Ecuatoriano de Seguridad Social (IESS), correos electrónicos institucionales, plataformas de pagos en línea, servicio de streaming, sistemas de gestión, entre otros.

  Nunca usar palabras comunes como “contraseña” o “1234” porque estas se encuentran en listas de contraseñas vulnerables en Internet que los ciberdelincuentes utilizan para vulnerar redes y equipos de manera remota.

- **Almacenamiento seguro de contraseñas:** No escribir contraseñas en notas del teléfono ni en papeles visibles. Se puede usar un gestor de contraseñas confiable como LastPass, Dashlane o Bitwarden.

- **Cambios regulares**: Cambiar contraseñas periódicamente. Se recomienda que esta acción se realice entre tres y seis meses, según la política interna o necesidad del establecimiento.

Protección de datos de Usuarios de Servicios Turísticos y el Establecimiento

- **No dejar información a la vista**: Documentos de los usuarios de servicios turísticos, detalles de pagos y datos personales deben guardarse en lugares seguros con acceso restringido.
- **Procesamiento de datos confidenciales**: La información de los usuarios de servicios turísticos debe compartirse únicamente con el personal autorizado. En caso de recibir llamadas o correos solicitando datos sensibles, se debe verificar la identidad de la persona antes de proporcionar cualquier información.

  Bajo ninguna circunstancia se deben fotografiar o fotocopiar tarjetas de débito o crédito.
- **Bloqueo de equipos móviles o de cómputo desatendidos:** Para evitar que personas no autorizadas ingresen a la información personal de usuarios de servicios turísticos o información corporativa del establecimiento, todo el personal debe tener como hábito mantener bloqueados los equipos cuando estén desatendidos, utilizando la combinación de las teclas **Windows**  **+ L**.

  Configurar el bloqueo automático: Evitar exponer la información contenida en los dispositivos configurando el bloqueo automático.

  Nota: Considerar el cumplimiento de lo que ordena la Ley Orgánica de Protección de Datos Personales del Ecuador.
- **Puertos USB:** Evitar el uso de los puertos USB de los computadores del establecimiento (Ej. recepción) para cargar dispositivos como celulares, tabletas, cámaras fotográficas, entre otros, pertenecientes a usuarios de servicios turísticos o personas externas. Este tipo de conexiones puede facilitar, de manera consciente o inconsciente, la instalación de software malicioso que comprometa la seguridad digital.

Uso seguro de terminales de pago (POS)

- **Inspeccionar el POS**: Revisar la terminal de pago antes de comenzar el turno para asegurarse de que no haya dispositivos extraños como 'skimmers'. Si se nota algo extraño, se debe notificar al supervisor inmediatamente.
- **Verificar transacciones**: Antes de realizar un cobro en plataformas digitales, confirmar el monto y los detalles con los titulares de las cuentas.

  Monitorear frecuentemente las transacciones realizadas y los reversos.
- **Limitar el acceso al POS**: Solo el personal autorizado debe operar el terminal de pago y evitar su uso por personas ajenas.

- **Uso seguro de Terminales de Pago**: Mantener los terminales de pago (POS) siempre a la vista del tarjetahabiente, de acuerdo con la Disposición General Quinta de la RESOLUCIÓN Nro. JPRM-2024-018-M (Junta de Política y Regulación Monetaria, 2024), para evitar posibles sanciones:

  "*QUINTA.- Los partícipes del Sistema Auxiliar de Pagos instruirán permanentemente a los comercios afiliados a su red de pagos que las transacciones presenciales con tarjetas de crédito, débito, prepago o billetera electrónica deberán realizarse a la vista del cliente.*"

  Evitar dejar los equipos desatendidos. Cuando no se están usando, estos equipos deben permanecer en un lugar seguro evitando manipulaciones no autorizadas.

  Se deben conocer los canales de comunicación de los proveedores de pago digital del establecimiento.

Detección de correos electrónicos y mensajes sospechosos

- **Correos Electrónicos Inusuales:** Se debe evitar abrirlos, marcarlos como spam y reportarlos al área correspondiente.
- **Identificación de phishing**: Se debe verificar la dirección de remitentes de correos electrónicos. Desconfiar si el dominio del correo no coincide con el nombre de la empresa o si existen faltas de ortografía en la redacción de los textos en las páginas que se navega.
- **Mensajes urgentes:** Desconfiar de solicitudes urgentes o de alarma donde se requieran datos personales o acciones que presionen a enviar información sensible, ya que podría tratarse de phishing. Siempre se debe verificar su autenticidad.
- **Enlaces sospechosos**: Antes de hacer clic en algún enlace, verificar el contexto del mensaje o correo electrónico, acercar el puntero del ratón al enlace donde se visualizará la dirección o URL completa. Si no se considera confiable, evitar ingresar al enlace y de ser el caso reportarlo.
- **Archivos adjuntos no esperados**: Marcar como spam y borrar el correo si proviene de una dirección desconocida. Si se reciben estos archivos de cuentas de un contacto conocido, comunicarse con el remitente por otra vía como llamando al número de teléfono que se tiene registrado. Considerar que existen herramientas de ingeniería social y con la incorporación de Inteligencia Artificial son capaces de simular sitios web de entidades, por lo que es importante verificar la autenticidad del remitente de manera adecuada.

Protección contra ataques de Ingeniería Social

- Evitar compartir datos confidenciales vía telefónica, plataformas de mensajería, correo o de manera física, sin verificar la identificación del solicitante. Si alguien pide acceso a sistemas, contraseñas, datos de usuarios de servicios turísticos o empleados, primero se debe verificar su identidad llamando a un número oficial que se conozca o confirmando con el supervisor. En lo posible, el establecimiento deberá contar con un procedimiento de actuación que contemple la interacción con el personal externo y/o prestador de servicios que incluya el listado de contactos oficiales para la gestión de dichos servicios.
- Desconfiar de urgencias sospechosas por cualquier medio: Si alguien ejerce presión para la obtención de determinada información diciendo: *"es urgente, necesitamos acceso ahora"*, verificarlo con un supervisor o llamar al número de contacto oficial.

Capacitación al Personal en Seguridad Digital

- **Cultura de Seguridad**: Proveer entrenamiento periódico en prevención de la ciberdelincuencia y buenas prácticas digitales abordando amenazas como phishing (fraude por correo electrónico), smishing (fraude por SMS) y ransomware (cifrado de datos con demanda de pago para su liberación), entre otras amenazas.
- **Protocolos de seguridad:** Promover la implementación de protocolos de seguridad en los sistemas generando confianza entre los compañeros de trabajo y principalmente en los usuarios de servicios turísticos que verán al establecimiento como un lugar seguro para sus actividades personales o profesionales.
- **Políticas para el manejo de datos sensibles:** Es importante que el personal esté capacitado en el manejo de datos sensibles, de acuerdo con la Normativa emitida en la Ley (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021), vigente en el Ecuador.
- **Capacitación técnica:** Si el establecimiento no cuenta en su nómina con personal del área de tecnologías, se recomienda contratar personal externo que realice las configuraciones necesarias y capacite al personal interno en buenas prácticas de seguridad digital y en el uso adecuado de los equipos. Ver Medidas de Seguridad y Protección de Sistemas.

Desactivación de Huéspedes que han dejado el Establecimiento

Al registrar la salida de huéspedes (check-out), el personal autorizado debe proceder a la desactivación de los permisos de acceso a la red Wi-Fi, lo que evita el acceso prolongado y no autorizado a los servicios digitales del establecimiento. Si se han facilitado dispositivos del establecimiento al usuario de servicios turísticos, se recomienda restablecerlos a su estado inicial mediante la herramienta de restauración o "*freeze*", que, al reiniciar, devuelve los dispositivos a su configuración predefinida, eliminando así cualquier cambio en la configuración o eliminación de información generada durante su uso.

Desactivación de personal que ha finalizado su relación laboral

Cuando un miembro del personal deja de laborar en el establecimiento, se deben revocar los accesos a sistemas y redes del establecimiento, incluyendo contraseñas de correo electrónico, redes Wi-Fi y cualquier otro sistema de servicios extras que preste el establecimiento. Es recomendable realizar revisiones internas periódicas, asegurándose que se han deshabilitado los permisos y cuentas del personal que ya no forme parte del establecimiento.

Nota: Deberían deshabilitarse todos los permisos y accesos de los usuarios que ya no formen parte del establecimiento, incluyendo el acceso a zonas restringidas del mismo.

Clasificación de riesgos por ciberdelitos

Una clasificación adecuada facilita la gestión de riesgos, priorizando la protección de información sensible y mejorando la respuesta ante incidentes.

Es recomendable mantener un documento de esta clasificación considerando sistemas, documentos, procesos, entre otros y adaptado a las necesidades del establecimiento, para que todos los colaboradores conozcan su importancia y gestionen adecuadamente según los niveles establecidos:

Riesgo Bajo (1-2): Involucran a elementos que son poco sensibles como encuestas de satisfacción, preferencias de usuarios de servicios turísticos, entre otros, cuyo uso indebido podría beneficiar a terceros y causar un impacto limitado. Es importante implementar controles básicos para precautelar el manejo adecuado de estos datos.

Riesgo Moderado (3-4): Involucran a plataformas, sistemas, información y procedimientos importantes para el funcionamiento del establecimiento como sistemas y registros de inventario, información logística, entre otros. Aunque no involucran datos altamente sensibles, si estos datos fueran comprometidos, podrían interrumpir las operaciones, causar errores en sistemas y/o facilitar el cometimiento

de delitos más graves por lo cual es necesario protegerlos para garantizar la continuidad de las operaciones y prevenir posibles pérdidas económicas.

Riesgo Alto (5-6): Involucran a plataformas, sistemas, información y procedimientos que incluyen datos personales, financieros u otra información sensible o confidencial, cuya exposición podría facilitar delitos graves como fraudes financieros, extorsión, suplantación de identidad, entre otros. Es fundamental proteger estos datos con controles de seguridad sólidos, ya que dichas vulnerabilidades podrían provocar graves consecuencias económicas o afectar la seguridad de las partes involucradas.

Riesgo Crítico (7-8): Involucran plataformas, sistemas, información y procedimientos que gestionan datos altamente sensibles de usuarios de servicios turísticos o del establecimiento. Esto incluye información de tarjetas de crédito y débito, credenciales de acceso y tokens bancarios, correos electrónicos asociados a cuentas financieras, accesos a sistemas y servidores, copias de seguridad, entre otros, cuya vulnerabilidad puede ocasionar fraudes financieros de gran impacto, deterioro en la imagen y pérdida de confianza de los usuarios de servicios turísticos que pueden acarrear graves consecuencias legales y económicas o incluso la paralización total de las operaciones.

El documento que contiene esta clasificación de riesgos puede establecer mecanismos de supervisión y monitoreo, previendo que los empleados cumplan con las medidas establecidas, para prevenir vulnerabilidades que pueden ser aprovechadas por los ciberdelincuentes. Adicionalmente, es importante considerar la normativa del Código Orgánico Integral Penal (COIP) (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014), el cual en su Art. 229 señala:

"*Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.* (...)"

2. Identificación de comportamientos sospechosos en el Establecimiento Turístico

Con el objetivo de proteger la seguridad de los usuarios de servicios turísticos, del personal y del establecimiento, es necesario mantenerse alerta ante cualquier actividad inusual. Algunos comportamientos aparentemente inofensivos podrían estar vinculados a delitos o ciberdelitos.

Aun cuando la anticipación de los comportamientos sospechosos puede ser limitada, a continuación, se presentan algunos eventos que el personal del establecimiento podría observar:

Acceso a lugares no autorizados o en horarios no habituales

Si se identifica a alguna persona en áreas restringidas o en horarios no permitidos, se debe notificar al supervisor y actuar de acuerdo al protocolo del establecimiento en términos de seguridad. Es importante que las reglas sean claras, visibles y socializadas tanto al personal como a los usuarios de servicios turísticos. En lo posible, el establecimiento deberá contar con un sistema de CCTV que permita registrar hechos anómalos y proporcionar indicios ante una posible investigación en caso de ser necesario.

Presión o intimidación al Personal

Los empleados deben conocer técnicas disuasivas verbales e informar de inmediato a su supervisor para evitar actuar bajo coacción. Es importante contar con un protocolo de actuación ante estos incidentes y capacitar al personal en su manejo adecuado.

Urgencias Inusuales

Si un usuario de servicios turísticos presenta una situación de urgencia poco clara o inusual, como insistir en obtener acceso inmediato a información o servicios sin justificación, el personal debe ser cauteloso y notificar a la administración.

Comportamientos anómalos de los sistemas

Los comportamientos extraños en los sistemas, como caídas inesperadas, lentitud excesiva o mensajes de error inusuales, deben ser reportados al departamento de tecnología, servicio técnico o al proveedor de servicios para una revisión oportuna.

Tráfico extraño en la Red Wi-Fi o lentitud excesiva

Existen herramientas de red que permiten automatizar el monitoreo y administración de las redes, las cuales pueden ser implementadas con el apoyo de un técnico calificado o por el proveedor del servicio de internet. Ante cualquier anomalía en la red se debe seguir el protocolo del establecimiento y notificar al personal de tecnología para identificar la causa y corregirla.

Situaciones Sospechosas con niñas, niños y adolescentes

En caso de que el personal del establecimiento de alojamiento turístico detecte alguna situación sospechosa que atente contra la integridad de niñas, niños y adolescentes, se deberá activar el protocolo de actuación conforme a lo dispuesto en el Acuerdo

Ministerial 2022-014 del Ministerio de Turismo que contiene el código de conducta para la prevención de la explotación sexual de niñas, niños y adolescentes, a fin de prevenir el cometimiento de un posible delito y deberá comunicarse de forma inmediata con el Sistema Integrado de Seguridad ECU 911 o al 1800 DELITO (1800 335 486).

Todo el personal debe estar capacitado para manejar estos incidentes de una manera adecuada y neutral a fin de no alertar a los posibles delincuentes mientras se toma contacto con la policía y/o autoridad. Ver la sección de Acciones ante situaciones sospechosas del presente documento.

3. Acciones ante actividades y comportamientos sospechosos

Anticipación frente a comportamientos sospechosos

Para mantener un entorno seguro y reducir los riesgos de ciberdelincuencia, los propietarios de establecimientos turísticos pueden establecer protocolos de seguridad y proporcionar entrenamiento periódico al personal para que estén en la capacidad de identificar delitos o ciberdelitos con base en esta guía, así como adoptar medidas disuasivas y prudentes, sin alertar a los sospechosos mientras se toma contacto con la autoridad competente.

Si se presenta alguna situación sospechosa como la presencia de adultos que no parecen tener una relación conocida o familiar con niñas, niños y adolescentes, actitudes evasivas o contradictorias, signos de incomodidad u otros, es necesario activar los protocolos de seguridad.

En lo posible, propietarios y empleados deben conocer al personal policial asignado al sector con el objetivo de generar acciones de seguridad ciudadana coordinadas ante cualquier situación de emergencia. Recuerde que la labor de la Policía Nacional es brindar protección y seguridad a la ciudadanía.

Se pueden generar acciones de trabajo periódicas con la Policía Nacional en el UPC más cercano, convocando a los propietarios y personal de los establecimientos del sector.

Comunicar la presunción de un delito

Ante cualquier presunción, notificar inmediatamente a la autoridad competente, con información detallada que facilite la investigación.

Es importante recordar que la complicidad y/o la omisión puede ser juzgada según lo establece el Código Orgánico Integral Penal de acuerdo con los siguientes artículos:

"Art. 43.- Cómplices.- Responderán como cómplices las personas que, en forma dolosa, faciliten o cooperen con actos secundarios, anteriores o simultáneos a la ejecución de una infracción penal, de tal forma que aun sin esos actos, la infracción se habría cometido. (...)

El cómplice será sancionado con una pena equivalente de un tercio a la mitad de aquella prevista para la o el autor".

"Art. 276.- Omisión de denuncia en razón de la profesión, cargo u oficio.- La persona que, en razón de profesión, cargo u oficio, en los ámbitos de educación, salud, recreación, religioso, deportivo o cultural, conozca de hechos que constituyan graves violaciones a los derechos humanos o delitos contra la integridad física, psicológica, sexual y reproductiva o muerte violenta de una persona y no denuncie el hecho, será sancionada con pena privativa de libertad de dos a seis meses.

Si la omisión es por parte de quien sea el propietario, responsable o representante legal de la institución pública o particular, se aplicará el máximo de la pena.

Si la omisión se produce sobre delitos contra la integridad física, psicológica o sexual de niños, niñas y adolescentes, se aplicará el máximo de la pena aumentada en un tercio.

No se podrá alegar secreto profesional y objeción de conciencia para justificar la falta de denuncia".

Denuncia formal de ciberdelitos en el Ecuador

Es fundamental denunciar de manera diligente ante cualquier indicio de riesgo o afectación significativa, especialmente si involucra menores o compromete información sensible.

En Ecuador, los ciberdelitos se denuncian en los UPC (Unidad de Policía Comunitaria), las oficinas de las Fiscalía General del Estado en todo el territorio nacional o accediendo al siguiente enlace: https://www.fiscalia.gob.ec/directorio-fiscalias/

Para realizar la denuncia se requiere la descripción del incidente, junto con cualquier evidencia que pueda aportar pruebas; la denuncia puede ser realizada por la víctima directa u otra persona. En lo posible se debe proporcionar los nombres de los implicados en el caso de conocerlos, junto con toda la información posible que facilite la investigación, como los hechos delictivos, las circunstancias (día, hora, lugar) y cualquier prueba disponible. El mayor nivel de detalle aumenta la efectividad de la investigación.

Medidas de Seguridad y Protección de Sistemas con asesoramiento especializado dirigido a Establecimientos Turísticos

Al implementar medidas de seguridad y protección tecnológica, debe considerarse el tipo de establecimiento, tamaño y capacidades, para determinar los procedimientos, protocolos y buenas prácticas que pueden adoptarse para una operación eficiente y segura (Kemp, 2023). Proveer servicios digitales de calidad favorece el bienestar de los usuarios de servicios turísticos, genera mayor confianza, fomenta el crecimiento del negocio y previene el cometimiento de ilícitos.

1. Acciones fundamentales para la seguridad de la red

Mantener actualizada una política sobre el uso de la red

Elaborar una política clara para el uso de la red interna y colocar un aviso visible en el establecimiento indicando que la red Wi-Fi está destinada exclusivamente a actividades legítimas. Además, se debe informar que las autoridades pueden requerir el monitoreo de la red en cualquier momento para prevenir actividades ilícitas. Este aviso actúa como un elemento disuasivo y refuerza la percepción de control y seguridad, haciendo menos probable que alguien intente utilizar la red para fines ilegales.

Cambio de la contraseña de la red Wi-Fi

La contraseña debe actualizarse periódicamente para asegurar que solo los usuarios tengan acceso a la red, reduciendo el riesgo de uso indebido o actividades ilícitas. Se debe utilizar una contraseña fácil de compartir con los usuarios, sin que resulte predecible, combinando letras, símbolos y números para mayor seguridad o a su vez con generación de códigos QR u otro método seguro.

Alternativas para la gestión de contraseñas de la red Wi-Fi

Una forma de mejorar la seguridad de la red Wi-Fi es implementar una página de autenticación con portal cautivo protegido con HTTPS, que permite un control seguro del acceso. Para esto, se requiere un router compatible.

Otra alternativa es utilizar un sistema de contraseñas dinámicas (Voucher System), que genera contraseñas temporales para los usuarios de servicios turísticos en forma de vouchers o códigos QR. Esto facilita la conexión y limita el acceso prolongado no autorizado.

Para establecimientos pequeños, una opción es el uso de páginas de bienvenida con contraseña compartida, donde los usuarios aceptan las políticas de uso antes de conectarse. Esta solución ofrece un nivel básico de seguridad y permite un control sencillo del acceso a la red.

Mantener software original

Es esencial mantener software original para contar con actualizaciones de seguridad permanentes. Las versiones no oficiales pueden introducir software malicioso que comprometa datos críticos. Adicionalmente, el uso de un antivirus comercial facilita el acceso a funcionalidades adicionales y mejores niveles de protección.

Configuración de alertas de tráfico de red

Configurar alertas que envíen notificaciones automáticas al correo electrónico en caso de picos inusuales de tráfico. Esto permite identificar actividades anómalas.

Ubicación de equipos informáticos y de comunicaciones en un lugar seguro

Ubicar los equipos en áreas restringidas que sean accesibles solo para el personal autorizado.

Desconexión de la red de usuarios de servicios turísticos fuera de horario

Si el negocio tiene horarios definidos de atención, se puede apagar el router fuera del horario establecido. Existen equipos que permiten programar esta función en horas específicas.

2. Protección de los Computadores del Establecimiento

Las cuentas de usuario individuales permiten a cada empleado trabajar de manera segura e independiente, con una contraseña personal que protege el acceso a la información que gestionan.

En Windows 11, se pueden seguir estos pasos para crear un nuevo usuario local y asignar una contraseña:

Creación de usuarios en Windows 11

Para la creación del usuario, se sugiere seguir los siguientes pasos que podrían variar ligeramente de acuerdo con la versión de Windows, en este caso Win11:

- Presiona las teclas **Windows** + **I** para abrir la ventana de configuración **(ver Ilustración 1)**.

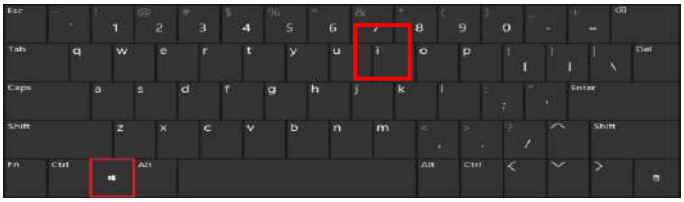

Ilustración 1 - Imagen de combinación de teclas.

Se desplegará la configuración del sistema operativo; luego continúa al siguiente paso.

- Selecciona "Cuentas" -> "Otros usuarios". Los textos pueden variar ligeramente debido a las versiones de Windows 11 **(ver Ilustración 2 y 3).**

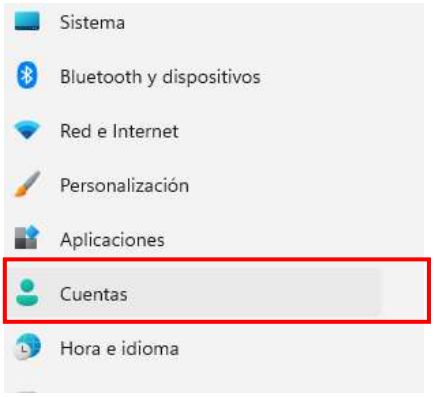

Ilustración 2- Creación de usuarios.

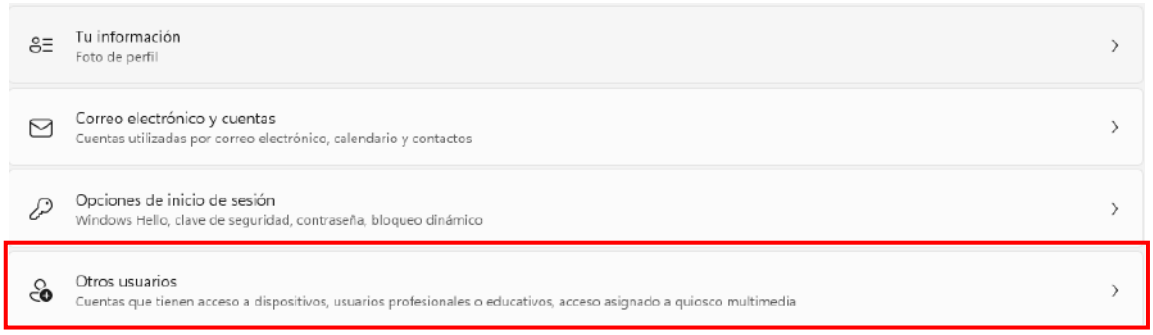

Ilustración 3 -Opción de usuarios adicionales al equipo.

- Se desplegará la siguiente ventana, bajo el apartado "Otros usuarios", haz clic en "Agregar otra persona a este equipo" **(ver Ilustración 4).**

Ilustración 4 - Creación de cuenta.

- Selecciona "No tengo la información de inicio de sesión de esta persona". Luego, elige "Agregar un usuario sin cuenta Microsoft". **Ilustración 5**.

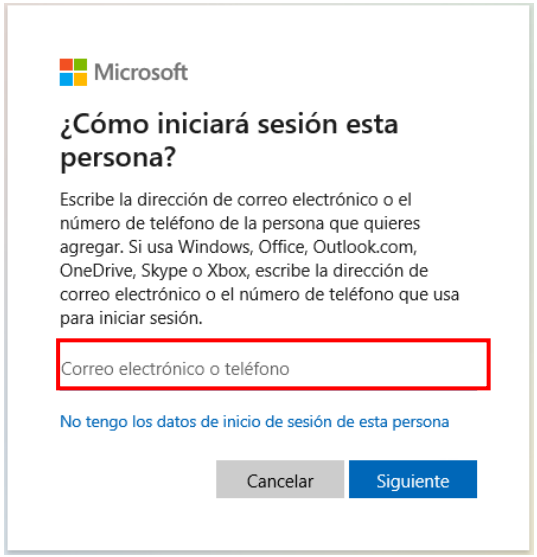

Ilustración 5 - Opción de configuración para creación de usuario con cuenta local.

- Ingresa el nombre de usuario y contraseña (mínimo 8 caracteres, incluyendo letras, números y símbolos). Opcionalmente, puedes agregar preguntas de seguridad para recuperar la cuenta en caso de olvidar la contraseña.
- Haz clic en Siguiente **(ver Ilustración 6)**.

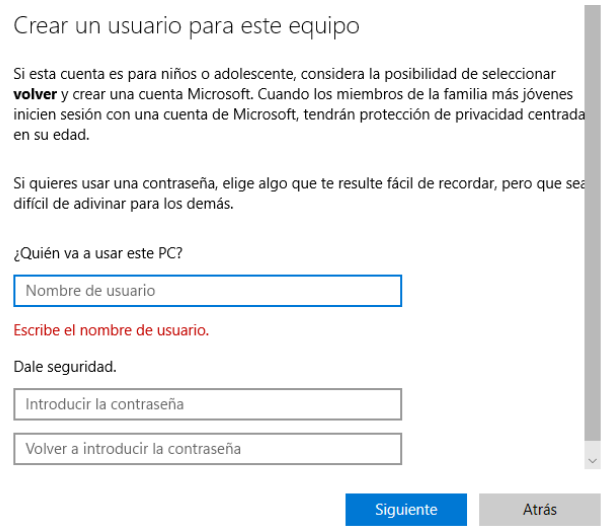

Ilustración 6 - Datos necesarios para la creación del usuario.

- Solo si es necesario, cambia para que el nuevo usuario sea administrador del equipo. En la lista, selecciona usuario, haz clic en "Cambiar el tipo de cuenta" y elige "Administrador" **(ver Ilustración 7)**.

Ilustración 7 - Opciones de cuenta del usuario creado.

Gestión centralizada de Usuarios

En establecimientos turísticos como hoteles, resorts, lodges, entre otros, se recomienda configurar un sistema centralizado como el directorio activo para gestionar todos los usuarios y equipos de cómputo. Esto permite administrar permisos, accesos y políticas de seguridad de forma eficiente a través de un software central. Esta configuración asegura mayor control y protección de la información. Consulta con personal de tecnología para implementar este sistema correctamente y adaptarlo a las necesidades del negocio.

3. Protección de Redes y Telecomunicaciones

Como propietario de un negocio, el objetivo principal es mantener la red segura y prevenir su uso en actividades ilegales. A continuación, se presentan algunas acciones simples y efectivas para proteger el establecimiento y a sus usuarios:

Configuración de Redes independientes para usuarios de servicios turísticos y para el personal del establecimiento

Una red dedicada para **usuarios de servicios turísticos,** permite ofrecer conectividad sin comprometer la seguridad de los sistemas internos, como la administración y los pagos, reduciendo los riesgos de ciberataques en un entorno de red controlado.

Red de usuarios de servicios turísticos: Configura una red Wi-Fi separada y exclusiva para el uso de los usuarios de servicios turísticos. Esta red no debe tener acceso a sistemas internos del establecimiento.

Red del Establecimiento: Configura una red privada y segura para operaciones internas (administración, pagos, etc.). Esta red debe estar restringida solo a personal autorizado y protegida con una contraseña robusta.

Al implementar redes WPA2 o WPA3 cifradas, es posible controlar el acceso y mantener separados los entornos de uso.

Los pasos para realizar su configuración son los siguientes:

1. **Acceder a la configuración del router**
    - Conectar la computadora o teléfono a la red del router (se puede usar Wi-Fi o un cable).
    - Abrir el navegador web y escribir la dirección IP de administración del router en la barra de direcciones (revisar el manual del router).
2. **Iniciar sesión en el router**
    - Introducir el nombre de usuario y la contraseña del router.
3. **Buscar la opción para crear una red de "invitados" en routers que lo permitan**
    - Una vez dentro de la configuración, buscar la sección para crear una red de invitados. Debe configurarse como "Huéspedes hotel", " Wi-Fi huéspedes" u otra.
    - Establecer una contraseña segura para la red, usando letras, números y caracteres especiales.

- Implementar una arquitectura de seguridad para que la red de invitados no disponga acceso a los dispositivos internos (como computadoras de trabajo).

4. **Configuración de una red separada para el personal**
    - Si ya se tiene una red solo para el personal, asegurarse de que esta mantenga una contraseña segura y difícil de predecir.
    - Si no existe una red separada para el personal, se debe configurar la opción de "Red principal" y establecer una contraseña fuerte.

Es importante asegurarse que la red del personal funcione correctamente y solo sea accesible al personal autorizado.

Implementación de Firewalls

Los firewalls son dispositivos o programas que controlan el tráfico de la red interna y el internet, actuando como barreras para filtrar el tráfico malicioso, bloquear accesos no autorizados y permitir solo el tráfico legítimo.

Los firewalls permiten proteger la red de cualquier organización, actuando como una primera línea de defensa frente a amenazas externas. Estos dispositivos o programas controlan el tráfico entrante y saliente, bloqueando posibles intentos de intrusión como contenido malicioso, ataques de malware o ransomware, además de restringir el acceso a sitios web que podrían poner en riesgo la red. **Ilustración 8**.

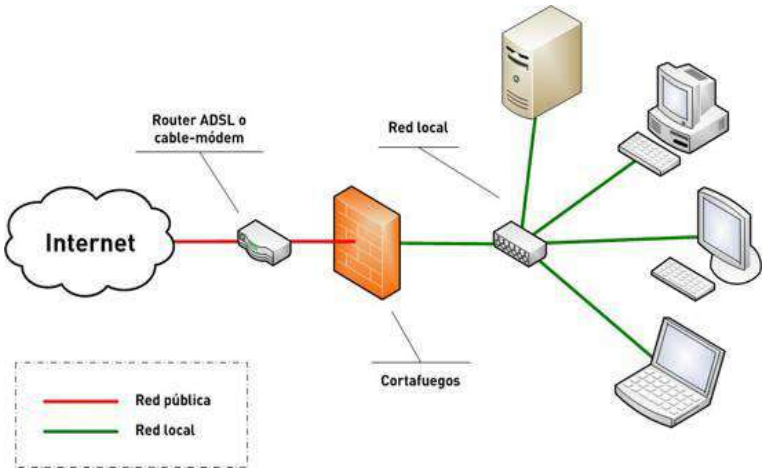

Ilustración 8 - Esquema de red - seguridad esencial de un firewall.

Sistemas de Detección de Intrusos

Un Sistema de Detección de Intrusos IDS es recomendable para establecimientos turísticos con redes complejas, como hoteles y resorts que manejan múltiples puntos de acceso. Si su negocio tiene estas características, un IDS ayuda a monitorear y bloquear actividades sospechosas antes de comprometer la red.

Cuando una red cuenta con muchos usuarios y puntos de acceso, se requiere un monitoreo activo en busca de cualquier actividad anormal que pueda indicar un ataque antes de que este cause daño, evitando interrupciones y protegiendo los datos como la información de los huéspedes o transacciones financieras.

Sistema de monitoreo y análisis de datos en tiempo real

Un sistema de monitoreo y análisis de datos en tiempo real permite recolectar, organizar y procesar grandes volúmenes de datos generados por diversas fuentes dentro de una empresa, como servidores, aplicaciones, dispositivos de red o sistemas de seguridad. Estos sistemas se utilizan para detectar eventos importantes, identificar anomalías y generar alertas que permitan una acción rápida ante incidentes o problemas.

Además, estas plataformas permiten crear visualizaciones y paneles que facilitan el análisis de tendencias y patrones, ayudando a los equipos de Tecnologías de la Información (TI) y Seguridad a tomar decisiones informadas. También pueden procesar grandes cantidades de información no estructurada o semiestructurada como registros (logs) y hacer que la información sea accesible y comprensible.

4. Actividades periódicas para prevenir riesgos de seguridad

Actualización del sistema operativo

Actualizar el sistema operativo como Windows y macOS, es una tarea necesaria para asegurar la protección y el buen rendimiento de tus dispositivos. Las actualizaciones incluyen las últimas correcciones de seguridad que previenen vulnerabilidades ante nuevas amenazas, añaden funcionalidades y corrigen errores. Automatizar este proceso garantiza que el equipo esté siempre al día, reduciendo riesgos y brindando una experiencia de usuario fluida.

En caso de que el dispositivo cuente con Windows 11, se sugiere realizar los siguientes pasos:

- Presionar las teclas **Windows** + **I** para abrir el menú de "Configuración".
- En el menú de la izquierda, hacer clic en "Windows Update" (puede estar al final de la lista).
- Hacer clic en el botón "Buscar actualizaciones". Si hay alguna actualización disponible, Windows comenzará a descargar automáticamente.

1. Instalar las actualizaciones
    - Una vez descargadas, selecciona "Instalar" si Windows no lo hace automáticamente.
    - Si se requiere, reiniciar la computadora para completar la instalación.
2. Activar las actualizaciones automáticas

- Asegurarse de activar la opción de actualización automática.

Ilustración 9 - Verificar activación de opción.

Actualización de la contraseña de administrador del router.

Cambiar regularmente la contraseña de administrador en el router permite proteger la infraestructura tecnológica. Usar contraseñas fuertes y actualizadas refuerza la seguridad y reduce considerablemente el riesgo de ataques.

Accede al router: El administrador debe conectarse con la dirección IP del Gateway o Puerta de enlace predeterminada para acceder a la página de configuración del router (generalmente 192.168.1.1) y las credenciales de acceso.

Cambia la contraseña: Localizar la opción "Administración" o "Security" y seleccionar "Cambiar contraseña". Se recomienda usar una contraseña segura que combine letras, números y símbolos, de mínimo 8 dígitos. Este proceso debe repetirse entre tres y seis meses.

NOTA: Los pasos pueden variar dependiendo del modelo del router y del proveedor de servicios contratado.

Se puede visualizar la puerta de enlace predeterminada (gateway) de la siguiente manera:

Presiona las teclas Windows + **R** para abrir la ventana de "Ejecutar".

Escribe el texto cmd y presiona la tecla Enter.

En la ventana negra, escribe ipconfig y presiona la tecla Enter.

Busca la línea que dice "Puerta de enlace predeterminada" o “Gateway” donde encontrarás la dirección IP del Gateway.

En la **Ilustración 10** se muestra el proceso:

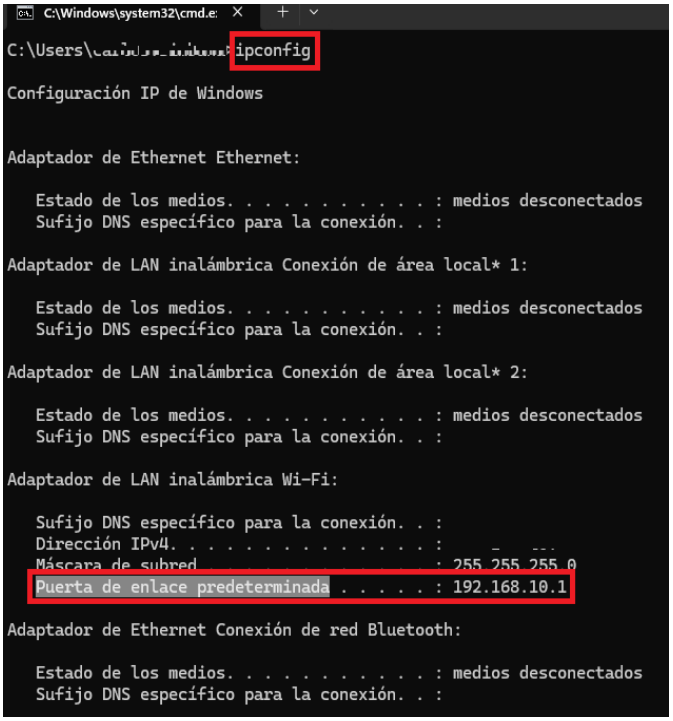

Ilustración 10 - Verificación de puerta de enlace.

Actualización del firmware

El firmware de dispositivos de red y servidores es el núcleo que asegura su funcionamiento óptimo. Mantenerlo actualizado corrige problemas de seguridad anteriores y mejora el rendimiento, lo que asegura que tus dispositivos continúen funcionando de manera eficiente, con menor riesgo de fallas o vulnerabilidades.

Actualización de software de aplicaciones

Mantener las aplicaciones y herramientas actualizadas es fundamental para asegurar su eficacia y proteger el sistema de posibles amenazas. Es recomendable utilizar las funciones de actualización dentro de cada aplicación o descargar las versiones más recientes desde las fuentes oficiales. Esto mejora el rendimiento de las aplicaciones y refuerza las medidas de seguridad ante nuevas vulnerabilidades que aparecen de manera continua.

Acciones de contingencia de seguridad

Desarrollar acciones de contingencia implica estar preparado para afrontar posibles incidentes. Los respaldos frecuentes de información crítica y los planes de recuperación son esenciales para asegurar la continuidad operativa. Definir protocolos claros para actuar ante ciberataques permite mitigar sus efectos de manera efectiva.

Auditorías de seguridad

Las auditorías de seguridad periódicas son herramientas clave para identificar y corregir vulnerabilidades en la infraestructura tecnológica. El monitoreo constante de sistemas y redes permite detectar conductas anómalas o riesgos antes de que se conviertan en incidentes. Para una protección exhaustiva, es importante contratar especialistas que realicen análisis de vulnerabilidades y pruebas de penetración que ofrezcan una capa adicional de seguridad.

Revisión y actualización periódica de medidas de seguridad

Las medidas de seguridad de la infraestructura tecnológica deben ser revisadas y adaptadas periódicamente para responder a nuevas amenazas. Evaluar los riesgos y actualizar las estrategias de protección permiten anticiparse a posibles ataques contra los sistemas informáticos.

Lista de Verificación para Establecimientos Turísticos

Se recomienda esta herramienta como una buena práctica para promover la seguridad en establecimientos turísticos. Puede adaptarse según las necesidades específicas de cada empresa:

Categoría	Descripción	☑ SI Cumple	✗ NO Cumple
Capacitación y Concienciación del Personal	**Capacitación del personal:** ¿El establecimiento cuenta con un plan de capacitación dirigido a empleados en prevención de incidentes y ciberdelitos?		
	Control y Protección de Datos: ¿El establecimiento capacita al personal en la Ley Orgánica de Protección de datos personales?		
	Medidas Preventivas y denuncias: ¿El personal está en la capacidad de ejecutar un plan preventivo y denunciar este tipo de ilícitos?		
Monitoreo y Control de Seguridad	**Auditorías periódicas:** ¿El establecimiento realiza revisiones de seguridad periódicas, tanto físicas como tecnológicas?		
	Control de accesos: ¿Conoce y monitorea los accesos físicos y lógicos a equipos y sistemas internos del establecimiento?		
	Protocolo de emergencia: ¿Cuenta con un plan ante incidentes de seguridad digital?		
	Registro de los errores: ¿Documenta y analiza incidentes para identificar causas, trazar soluciones y mejorar la seguridad digital?		
Seguridad para los Clientes	**Acciones de Sensibilización:** ¿Informa a sus clientes sobre el uso seguro de redes y dispositivos?		
	Mejorar su seguridad: ¿Cuenta con políticas de seguridad digital como el doble factor de autenticación en sus dispositivos?		
	Wi-Fi público (Precaución): ¿Recomienda a los clientes priorizar el uso de su plan de datos móviles para transacciones en línea o conectarse a la red Wi-Fi segura del establecimiento, evitando el uso de redes abiertas en plazas o calles?		
Protección de Datos y Seguridad	**Política: ¿**Cuenta con una política de protección de datos personales en el establecimiento?		
	Contraseñas robustas: ¿Usa claves con letras, números y símbolos en todos los dispositivos del establecimiento?		

Categoría	Descripción	☑ SI Cumple	✖ NO Cumple
	Doble capa de seguridad: ¿Tiene habilitado la autenticación multifactor (MFA) en sus dispositivos?		
	Protección de datos: ¿Gestiona su información confidencial bajo medidas de seguridad y acceso autorizado?		
	Uso de puertos USB: ¿Restringe el uso de memorias y dispositivos USB personales, en los equipos del establecimiento?		
	Revocatoria de permisos: ¿Revoca accesos cuando alguien deja de trabajar en la Empresa?		
	Respaldos: ¿Respalda la información periódicamente de preferencia en una ubicación externa fuera del Establecimiento?		
Seguridad en Redes y Dispositivos	**Redes independientes seguras:** ¿Usa redes separadas o privadas para clientes y empleados?		
	Cortafuegos activo: ¿Cuenta con firewall para bloquear accesos no autorizados?		
	Contraseñas propias seguras: ¿Cambia contraseñas predeterminadas o por defecto de routers y equipos informáticos?		
	Actualización de contraseñas: ¿Actualiza o cambia las claves de los equipos y sistemas regularmente?		
	Monitoreo de la red: ¿Cuenta con un Sistema de Detección de Intrusos (IDS) para identificar ataques?		
	Navegación segura: ¿Usa una VPN para acceso remoto de los empleados y servicios?		
	Actualización del software de la Empresa: ¿Actualiza regularmente el firmware de routers y equipos?		
	Uso de los Dispositivos de Pago (POS): ¿Cuenta con personal designado para el uso autorizado de los terminales de pago?		
	Verifica cada transacción: ¿Procesa pagos con presencia y confirmación del tarjetahabiente?		
	CCTV: ¿Cuenta con sistema de circuito cerrado de vigilancia?		

Glosario

Android: Sistema operativo móvil de Google usado por múltiples fabricantes.

Auditoría de seguridad: Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones. (INCIBE, Glosario de Términos de Ciberseguridad, 2020)

Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtración de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos. (INCIBE, Glosario de Términos de Ciberseguridad, 2020)

Ciberdelito: Conducta típica, antijurídica y culposa mediante la utilización de cualquier medio tecnológico, dispositivo informático, electrónico o tecnología digital, que ponga en peligro la seguridad de los activos de los sistemas de información o comunicación, de los bienes jurídicos personales o cualquier otro bien jurídico protegido. (Proyecto de Estrategia Nacional contra la Ciberdelincuencia, 2024).

Los ciberdelitos incluyen una variedad de acciones ilícitas que se cometen a través de medios digitales. Entre los principales se encuentran:

- **Ciberacoso / Ciberbullying:** El ciberacoso puede incluir la difusión de rumores, la publicación de información falsa o de mensajes desagradables o comentarios o fotos vergonzosos, o bien excluir a alguien de las redes en línea. A menudo son el resultado de la interacción personal en la escuela u otros espacios sociales, y pueden causar daños profundos, ya que pueden afectar a los niños víctimas en todo momento y llegar rápidamente a un público muy amplio (Naciones Unidas, 2014).

- **Grooming:** El grooming es la situación en la que un adulto acosa sexualmente a un niño, niña o adolescente mediante el uso de plataformas digitales. El acosador suele mentir sobre su identidad, generar un vínculo de amistad y confianza con la potencial víctima y luego pedirle información íntima como una foto o un video. Luego suele extorsionarlo con difundir ese material si no accede a un encuentro personal o a enviar más imágenes (UNICEF Argentina, s.f.).

- **Ingeniería social:** Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten

valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

- **Intrusión:** Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para acceder a un área o dispositivo sin autorización, con el objetivo de realizar actividades ilegítimas. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

- **Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. (INCIBE, Glosario de Términos de Ciberseguridad, 2020)

- **Phishing / Smishing:** Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

- **Ransomware:** Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

- **Suplantación de identidad:** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (ciberbullying). Como ejemplo es cuando en las redes sociales se crea un perfil de otra persona e interactúa con otros usuarios haciéndose pasar por ella. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

- **Sexting / Exposición de sí mismo:** Consiste en enviar fotografías o vídeos producidos por uno mismo con connotación sexual, desde el teléfono móvil u otro dispositivo con cámara. El riesgo está en que, una vez enviados estos contenidos, pueden ser utilizados de forma dañina por otras personas (INCIBE, https://www.incibe.es/menores/tematicas/sexting, s.f.).

  El sexting se distingue de otras prácticas por ciertas características:

  - Voluntariedad. Los mensajes, imágenes y videos son creados conscientemente por sus protagonistas y enviados inicialmente por ellos mismos a otras personas.

- Carácter sexual. Los contenidos tienen una clara connotación sexual: desnudez o semidesnudos, así como muestra o descripción de actividades sexuales.

- Uso de dispositivos tecnológicos. Lo más habitual es que la víctima utilice su móvil o smartphone, aunque también puede darse la comunicación usando la webcam de la Tablet, el ordenador portátil o de sobremesa. Cuando esto sucede durante una videollamada o una sesión de chat con webcam, se denomina sexcasting.

Ciberseguridad / Seguridad digital: Protección de la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos a fin de mejorar la seguridad, la resiliencia, la fiabilidad y la confianza en las TIC. El concepto habitualmente abarca dimensiones políticas (intereses nacionales y seguridad), técnicas y administrativas (Cross, Hirrle , & Lim , 2021).

Cifrado: Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado. La confidencialidad de la información es un pilar fundamental de la seguridad digital. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Control Parental: Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet.

Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Criticidad: Atributo que mide el riesgo que provoca un comportamiento erróneo o negligente respecto a las condiciones normales de funcionamiento al que está sometido un proceso, sistema o equipo. A mayor nivel de criticidad, mayor gravedad de los hechos ocurridos. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Datos personales: Información relativa a una persona física viva que puede ser identificada o identificable a través de la recopilación de una serie de datos de carácter

personal, que establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Digitalización: Es el uso de tecnologías y datos digitales y las interconexiones entre ellos, que dan lugar a nuevas actividades o a cambios en las actividades existentes (IMF, OECD, WTO, & UN, 2023).

Doble factor de autenticación: Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Firewall / Cortafuegos: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación.

Estos sistemas suelen poseer características de privacidad y autentificación (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Gestor de contraseñas: Programa o aplicación que se puede integrar en los principales navegadores y que permite generar contraseñas robustas y almacenarlas cifradas junto con los nombres de usuario para diferentes sitios web y aplicaciones, con la facilidad de tener que recordar solo la contraseña de acceso al gestor. Esto permite tener diferentes contraseñas por cada sitio para incrementar así la seguridad. Algunos de ellos ofrecen además servicios adicionales, como el autocompletado de datos personales, servicios en la nube y autenticación de doble factor para acceder a las contraseñas almacenadas (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

HTTPS: Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés Hypertext Transfer Protocol Secure, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

IDS: Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Inteligencia Artificial: Conocida como IA por sus siglas, son sistemas informáticos diseñados para imitar y replicar algunas capacidades cognitivas humanas, como el aprendizaje, la percepción, el razonamiento y la toma de decisiones. Esta tecnología se basa en algoritmos complejos y utiliza grandes cantidades de datos para realizar tareas específicas (INCIBE, s.f.).

iOS: Sistema operativo móvil de Apple usado de uso exclusivo de los dispositivos Apple.

Log / Logs: Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/ salida de sesión, tiempo de actividad o conexiones, entre otros.

Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

macOS: Sistema operativo de Apple para las computadoras personales de Apple.

Pasarela de pagos: Plataforma tecnológica que permite a los establecimientos aceptar pagos electrónicos. Actúa como un intermediario entre los establecimientos y los proveedores de servicios de pago, facilitando la transmisión segura de la información del pago y la autorización de la transacción (Junta de Política y Regulación Monetaria, 2024).

Política de seguridad: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Protección de Datos: Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar (RAE, s.f.).

Redes Públicas o Abiertas: Se trata de conexiones, generalmente inalámbricas, disponibles en lugares como cafeterías, aeropuertos o centros comerciales. Son útiles, pero también pueden ser peligrosas. Suelen carecer de medidas suficientes de seguridad y cualquiera puede conectarse a ellas. Esto significa que tu información podría ser interceptada por personas malintencionadas (INCIBE, Instituto Nacional de Ciberseguridad, s.f.).

Red LAN: Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Red WAN: Una red de área amplia, o WAN (Wide Area Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Riesgo: Una medida del grado en que una entidad se ve amenazada por una circunstancia o evento potencial, y típicamente una función de: (i) los impactos adversos que surgirían si la circunstancia o evento ocurre; y (ii) la probabilidad de ocurrencia (NIST, s.f.).

Router: Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es).

En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del proveedor de Internet.

El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Servidor: Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla.

Algunos ejemplos de servidores son los que proporcionan el alojamiento de sitios web y los que proporcionan el servicio de envío, reenvío y recepción de correos electrónicos. (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Skimmer: Este término proviene del inglés, to skim (leer rápidamente u hojear), por lo que los delincuentes cuentan con diferentes dispositivos, conocidos como skimmers, para apropiarse de los datos sin que la víctima se dé cuenta. Generalmente, se lleva a cabo al realizar transacciones en un cajero automático o pagar en un terminal de punto de venta manipulado previamente (SANTANDER, 2023).

SMS (servicio de mensaje corto): Servicio de telefonía que permite enviar y recibir mensajes que se escriben en la pantalla de un teléfono celular. (https://dle.rae.es, s.f.)

Software: Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El software conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Terminales de pago (point of sale - POS): Se refiere al dispositivo o terminal para uso de tarjetas de pago (crédito o débito) en un establecimiento (punto de venta) (CPSS & BIS, 2003).

TI: Tecnologías de la Información

TIC: Tecnologías de la Información y Comunicaciones.

Transacción: Trato, convenio o negocio. Contrato por el cual las partes, dando, prometiendo o reteniendo cada una alguna cosa, evitan la provocación de un pleito o ponen término al que había comenzado (RAE, s.f.).

Transacción electrónica: Intercambio de carácter comercial o no comercial que se realizan a través de medios electrónicos, es decir, mediante el intercambio de mensajes de datos. “Mensaje de datos” significa información generada, enviada, recibida o almacenada por medios electrónicos, ópticos o similares (ESCAP, UN UNCITRAL, & EIF).

UPC: Unidad de Policía Comunitaria.

VPN: Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura

gracias al cifrado de la comunicación (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Wi-Fi: Es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto, de una red LAN que no utiliza un cable físico para el envío de la información (INCIBE, Glosario de Términos de Ciberseguridad, 2020).

Windows: Sistema operativo de Microsoft para computadoras personales.

WPA (Wi-Fi Protected Access): En español, acceso protegido inalámbrico, consiste en un sistema usado en el ámbito de las comunicaciones inalámbricas destinado a evitar que cualquier persona no expresamente autorizada pueda acceder a la red mediante el uso de este algoritmo de cifrado (Seguridad en redes wifi: una guía de aproximación para el empresario, 2019).

WPA2 (Wi-Fi Protected Access 2): En español Acceso Wi-Fi protegido 2, a su vez es un sistema que se creó para corregir las deficiencias del sistema previo, WPA. (Seguridad en redes wifi: una guía de aproximación para el empresario, 2019).

WPA3 (Wi-Fi Protected Access 3): Es un protocolo más seguro y robusto que WPA2, ya que resuelve algunas de sus vulnerabilidades y proporcionar un mayor nivel de seguridad para las redes Wi-Fi. (Seguridad en redes wifi: una guía de aproximación para el empresario, 2019).

Referencias

Asamblea Constituyente del Ecuador. (2008). *Constitucion de la República del Ecuador*. Montecristi - Manabi: Registro Oficial No.449.

Asamblea Nacional del Ecuador. (2002). *Ley de Turismo*. Quito - Ecuador: Registro Oficial No.733.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Quito – Ecuador: Registro Oficial No.180.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Quito – Ecuador: Registro Oficial No.459.

CPSS, & BIS. (2003). *A glossary of terms used in payments and settlement systems*. Obtenido de https://www.bis.org/cpmi/glossary_030301.pdf

Cross, S., Hirrle , S., & Lim , M.-A. (2021). *Guía sobre la Estrategia Nacional contra la Ciberdelincuencia*. INTERPOL.

ESCAP, UN UNCITRAL, & EIF. (s.f.). *Guía De Evaluación De La Preparación Legal*. Obtenido de https://readiness.digitalizetrade.org/es/legal-guide/ia-general-principles

https://dle.rae.es. (s.f.).

https://dpej.rae.es/lema/transacci%C3%B3n. (s.f.).

https://servicios.turismo.gob.ec/catastro-turistico/. (Enero de 2025).

IBM Security. (2024). *IBM X-Force Threat Intelligence Index 2024*. Obtenido de https://verizon.com/dbir: https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

IMF, OECD, WTO, & UN. (2023). *Handbook on Measuring Digital Trade (Second Edition)*. Secretaría WTO.

INCIBE. (s.f.). Obtenido de https://www.incibe.es/ciudadania/blog/inteligencia-artificial-ia-que-es-ventajas-y-riesgos

INCIBE. (2020). *Glosario de Términos de Ciberseguridad*.

INCIBE. (s.f.). *https://www.incibe.es/menores/tematicas/sexting*.

INCIBE. (s.f.). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/node/506666

Juca-Maldonado, F., & Medina-Peña, R. (2023). *Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. Revista Portal de la Ciencia*. Obtenido de https://doi.org/10.51247/pdlc.v4i3.394.

Junta de Política y Regulación Monetaria. (2024). *Resolución Nro. JPRM-2024-018-M*. Quito – Ecuador.

Kemp, S. (2023). *Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. Computers & Security*.

Mentsiev, A., Engel, M., & Tsamaev, A. (2020). *https://doi.org/10.1088/1755-1315/272/2/022001*.

Naciones Unidas. (2014). *Informe anual de la Representante Especial del Secretario General sobre la violencia contra los niños*.

NIST. (s.f.). *Computer Security Resource Center*. Obtenido de https://csrc.nist.gov/glossary/

Parder, M., Gryffroy, p., & Juurik, M. (2024). *Ethical considerations in a pan-European project targeting adolescent cybercrime prevention*. Obtenido de https://doi.org/10.1177/17470161241247803.

RAE. (s.f.). *Diccionario Panhispánico del español jurídico*. Obtenido de https://dpej.rae.es/

Ruslan, M. (2024). *Mitigating Financial Fraud and Cybercrime: A Systematic Literature Study. Accounting Studies and Tax Journal*.

SANTANDER. (2023). *https://www.santander.com/es/stories/skimming*.

(2019). *Seguridad en redes wifi: una guía de aproximación para el empresario*. INCIBE (España).

UNICEF Argentina. (s.f.). *https://www.unicef.org/argentina/el-grooming-es-un-delito*.

Firmas de Responsabilidad

Nombre y Cargo	Firma
Elaborado por: Ing. Diego Tejada C. Analista de Ciberdelitos 2	Firmado electrónicamente por: DIEGO ARMANDO TEJADA CAMPOS
Mgs. Carlos Simbaña C. Analista de Ciberdelitos 2	Firmado electrónicamente por: CARLOS MARCELO SIMBANA COBA
Revisado por: Mgs. Fernando Moya L. Especialista de Ciberdelitos	Firmado electrónicamente por: FERNANDO ANDRES MOYA LEIMBERG
Ing. Freddy Gallardo S. Especialista de Ciberdelitos	Firmado electrónicamente por: FREDDY GUSTAVO GALLARDO SOSA
Mgs. Jorge Néjer G. Especialista de Ciberdelitos	Firmado electrónicamente por: JORGE MAURICIO NEJER GUERRERO
Mgs. Gabriel Reinoso M. Analista de Ciberdelitos 2	Firmado electrónicamente por: GABRIEL ANDRES REINOSO MARTINEZ
Revisado y avalado por: Mgs. Fernando Illescas P. Director de Ciberdelitos	Firmado electrónicamente por: JORGE FERNANDO ILLESCAS PENA
Aprobado por: TCnl. (SP) Luis Pérez D. Subsecretario de Combate al Delito	Firmado electrónicamente por: LUIS FERNANDO PEREZ DAVILA