MICROONDAS ACCESO FIBRA EN TELECOMUNICACIONES S.A. DE C.V.

Política

SEGURIDAD DE LA INFORMACIÓN

Clave: **PO-05**

Versión: **01**

Entrada en vigor: **16-oct-24**

Elaboró	Revisó	Aprobó
José Fernando León CEO	**Ana María Cruz** Administrador de Proyectos **Praxedes Orduño** Administrativo Contable y de Recursos Humanos **Diego Hernández** Coordinador de Proyectos Huawei-Bestel	**José Fernando León** CEO

Este documento es propiedad de **Microondas Acceso Fibra en Telecomunicaciones S.A. de C.V.** y es exclusivo para uso interno. La única versión oficial de este documento es la digital disponible en la plataforma de gestión documental. La organización no se hace responsable de las copias impresas de la misma, salvo que sean copias controladas.

1 Todos los miembros de la organización deben observar la presente política para salvaguardar la información de la organización y sus partes interesadas. Los controles establecidos en esta política están basados en la evaluación de riesgos a la SI que dio como resultado la **RE-09 Declaratoria de aplicabilidad**. Cada apartado hace referencia al control operacional específico establecido por el anexo A de la Norma Internacional ISO/IEC 27001:2022.

2 Sobre la seguridad de la información.

2.1 Generalidades.

2.1.1 Políticas de seguridad de la información (A.5.1).

Esta política se divide en secciones temáticas que agrupan los controles aplicables de la declaratoria de aplicabilidad por afinidad conceptual. Las secciones de la presente son:

2.1.1.1 Sobre la gestión de la información.

2.1.1.2 Sobre la infraestructura de la información.

2.1.1.3 Sobre los eventos de la información.

2.1.2 Procedimientos operativos documentados (A.5.37).

2.1.2.1 La organización debe establecer manuales e instructivos específicos para las actividades que constituyan un proceso con sus respectivas entradas, salidas y controles.

2.1.2.2 En aras de la practicidad y esbeltez documental, los lineamientos que no impliquen un proceso, no deben traducirse en procedimientos.

2.1.3 Cumplimiento de políticas, normas y estándares de seguridad de la información (A.5.36).

2.1.3.1 Esta política es de cumplimiento obligatorio para todos los colaboradores cubiertos por el alcance del SGI.

2.1.3.2 Si la organización decidiera implementar otras normas o esquemas de certificación en materia de seguridad de la información, esta debe darle máxima prioridad a los requisitos establecidos por la versión vigente de ISO/IEC 27001 y otros documentos emitidos por ISO o IEC.

2.2 Requisitos a considerar.

2.2.1 Requisitos legales, estatutarios, reglamentarios y contractuales (A.5.31).

2.2.1.1 La organización debe conocer todos los requisitos legales y reglamentarios en materia de seguridad de la información que le apliquen, destacando la Ley Federal de Protección de Datos Personales en Posesión de Particulares y los requisitos contractuales de confidencialidad que cada cliente y parte interesada establezcan.

2.2.1.2 La organización debe asegurar el cumplimiento de todos los requisitos de seguridad de la información de sus partes interesadas, salvo cuando estos contravengan las disposiciones de la versión vigente de ISO/IEC 27001 u otras emitidas por ISO o IEC.

3 Sobre la gestión de la información.

3.1 Control de los activos de información.

3.1.1 Clasificación de la información (A.5.12).

3.1.1.1 Se consideran activos de información de la organización a aquellos que puedan estar sujetos a requisitos específicos de seguridad de la información, por ejemplo, aquellos amparados bajo convenios de confidencialidad y aquellos con datos personales.

3.1.1.2 La información debe ser clasificada como alguna de las siguientes:

3.1.1.2.1 Pública, que no tiene restricción alguna de acceso. Por ejemplo: políticas relacionadas con los proveedores de la organización.

3.1.1.2.2 Uso interno, cuyo acceso por personas ajenas a la organización es inútil o inconveniente. Por ejemplo: procedimientos de operación.

3.1.1.2.3 Confidencial, que contiene información protegida por algún requisito legal u otro aplicable y solo debe ser usada para fines específicos, así como vista por los responsables de esos fines específicos. Por ejemplo: información protegida contractualmente o expedientes de los trabajadores.

3.1.2 Etiquetado de información (A.5.13).

3.1.2.1 La información documentada debe ser etiquetada mediante la "Clasificación de Documentos" de aDhOC System®, cuando esto no sea posible o conveniente —por ejemplo, cuando el documento en cuestión se use completamente fuera de la plataforma— el documento deberá ser etiquetado con la clasificación correspondiente en marca de agua, solo si fuera de uso interno o confidencial.

3.1.3 Inventario de información y otros activos asociados (A.5.9).

3.1.3.1 Cada usuario debe tener su información nombrada y organizada de manera que pueda saber en cualquier momento qué tanta información resguarda. Cada usuario puede usar los crtierios de organización y las carpetas que considere pertinentes siempre que sea capaz de ubicar cualquier archivo con rapidez y claridad.

3.1.4 Copia de seguridad de la información (A.8.13).

3.1.4.1 Todos los usuarios deben tener al menos un respaldo de toda la información del disco duro de su equipo, exceptuando archivos del sistema y otros que no sean parte de las operaciones de la organización.

3.1.4.2 Los respaldos pueden ser hechos en medios físicos de almacenamiento externo o en la nube, dando preferencia a esta última.

3.1.4.3 Los respaldos deben ser renovados cuando menos una vez por cada mes calendario.

3.2 Control de los usuarios de la información.

3.2.1 Roles de seguridad de la información y responsabilidades (A.5.2).

3.2.1.1 Todos los usuarios son responsables de la información bajo su control.

3.2.1.2 Solo el CEO y su primera línea de reporte pueden ser los dueños de los riesgos a la SI.

3.2.2 Segregación de deberes (A.5.3).

3.2.2.1 Los descriptivos de puesto no deben incluir funciones que se contradigan entre sí ni que contradigan u obstaculicen las funciones de otros roles.

3.2.3 Responsabilidades de gestión (A.5.4).

3.2.3.1 Todos los colaboradores de la organización deben:

3.2.3.1.1 Conocer esta política.

3.2.3.1.2 Aclarar a través del rol mencionado en 3.2.1.1 cualquier duda, inquietud o sospecha que pudieran tener en materia de SI.

3.2.3.2 El rol de "coordinador de proyectos (Huawei-Bestel)" tendrá a su cargo la gestión operativa de la seguridad de la información y será responsable de informar a la alta dirección del desempeño de la organización en la materia. Tal persona será conocida como "responsable de seguridad de la información".

3.2.4 Términos y condiciones de empleo (A.6.2).

3.2.4.1 Los descriptivos de puesto de todos los colaboradores de la organización deben contener el requisito de cumplir con esta política y con la política del sistema de gestión integrado.

3.2.5 Acuerdos de confidencialidad o no divulgación (A.6.6).

3.2.5.1 Los contratos laborales de todos los colaboradores que ingresen a partir de la entrada en vigor de esta política deben incluir el compromiso de asegurar la no divulgación de la información de la organización hacia partes externas, exceptuando aquellas justificables como los clientes mismos o las autoridades.

3.2.5.2 La organización debe suscribir y honrar estrictamente todos los convenios de confidencialidad solicitados por sus clientes y otras partes interesadas, siempre que no interfieran o superen sus capacidades operativas.

3.2.6 Concientización, educación y capacitación en seguridad de la información (A.6.3).

3.2.6.1 El comité del SGI debe ser capacitado en la interpretación de la norma internacional ISO/IEC 27001 en su versión vigente.

3.2.6.2 Los controles de seguridad de la información pueden ser reforzados mediante cualquier medio que resulte práctico, incluyendo cursos, pláticas cortas, folletos, videos y cualquier material físico o virtual de difusión.

3.2.7 Proceso disciplinario (A.6.4).

3.2.7.1 Cuando se sospeche que alguien ha incurrido en una falta a cualquiera de los preceptos de esta política, el responsable de seguridad de la información debe:

3.2.7.1.1 Determinar si existe suficiente evidencia para demostrar inequívocamente que la falta ocurrió.

3.2.7.1.2 Si la falta quedara demostrada, presentarla ante la alta dirección junto con toda la evidencia aplicable.

3.2.7.2 Cuando una falta a cualquiera de los preceptos de esta política sea demostrada, la alta dirección debe seleccionar y ejecutar, a su criterio y respetando el principio de proporcionalidad, una de las siguientes sanciones, ordenadas de manera ascendente:

3.2.7.2.1 Una llamada de atención por escrito.

3.2.7.2.2 Una llamada de atención por escrito y la obligación de tomar una plática o curso de concientización de al menos una hora en la materia que diera origen a la falta.

3.2.7.2.3 Un día de suspensión laboral.

3.2.7.2.4 Rescisión del contrato laboral.

3.2.7.2.5 Rescisión del contrato laboral y demandas legales procedentes.

3.2.7.3 Cuando se demuestre la reincidencia de una persona en una falta de la misma naturaleza, la sanción seleccionada para tal reincidencia debe ser mayor que la seleccionada para las incidencias anteriores.

3.2.8 Responsabilidades después de la terminación o cambio de empleo (A.6.5).

3.2.8.1 Los contratos laborales de todos los colaboradores que ingresen a partir de la entrada en vigor de esta política deben incluir el compromiso de asegurar la no divulgación de la información de la organización hacia partes externas una vez terminada la relación laboral y sin límite de tiempo.

3.3 Control de los accesos a la información.

3.3.1 Gestión de identidad (A.5.16).

3.3.1.1 Todos los usuarios deben tener usuario y contraseña para ingresar a sus equipos y plataformas de almacenamiento de información.

3.3.1.2 Los nombres de usuario para todos los aplicativos deben coincidir con o hacer referencia al nombre de la persona propietaria.

3.3.1.3 Los usuarios no deben compartir sus accesos con otras personas, bajo ninguna circunstancia.

3.3.1.4 Los usuarios son completamente responsables de todas las actividades realizadas en cualquier activo de procesamiento de información bajo su nombre de usuario. Esta responsabilidad no puede ser compartida ni distribuida con otras personas.

3.3.2 Información de autenticación (A.5.17).

3.3.2.1 El responsable de seguridad de la información debe tener registro de todos los usuarios activos con acceso a información de la organización. Esta información debe estar actualizada en todo momento.

3.3.3 Derechos de acceso (A. 5.1).

3.3.3.1 Solo deben tener acceso a la información las personas que puedan necesitarla para sus funciones.

3.3.3.2 Solo deben tener acceso a los datos personales de los colaboradores, incluyendo los asentados en formatos, contratos y otros documentos, los colaboradores de la Gerencia Administrativa.

3.3.3.3 Solo debe tener acceso a un equipo de cómputo la persona a la que tal equipo ha sido asignado. Esto incluye computadoras, celulares y otros equipos de procesamiento de información. Queda estrictamente prohibido intercambiar o prestar equipos.

3.3.4 Derechos de acceso privilegiado (A.8.2).

3.3.4.1 Los derechos de acceso privilegiado se deben otorgar únicamente a individuos autorizados que requieran de tal acceso para el desempeño de sus funciones laborales y basándose en el principio del menor privilegios, es decir, se otorgarán los permisos mínimos necesarios para realizar una tarea específica.

3.3.4.2 Los derechos de acceso privilegiado solo se deben otorgar bajo demanda y para la realización de mantenimientos y funciones específicas. Al término de las funciones, los derechos de acceso privilegiado deben ser revocados inmediatamente.

3.3.4.3 La alta dirección debe autorizar todos los derechos de acceso privilegiado y constatar su revocación.

3.3.5 Control de acceso (A.5.15).

3.3.5.1 Toda la información almacenada por la organización debe estar protegida y debe ser únicamente accesible a los colaboradores con los derechos de acceso adecuados y que cuenten con la información de autenticación correspondiente.

3.3.5.2 Todos los equipos de cómputo deben estar configurados para bloquearse automáticamente después de un período de inactividad de 5 minutos.

3.3.6 Entrada física (A.7.2).

3.3.6.1 El ingreso a las instalaciones de la organización debe ser controlado.

3.3.6.2 Solamente los colaboradores y partes interesadas externas con autorización justificada de algún colaborador deben tener acceso a las instalaciones de la organización.

3.3.6.3 La organización debe implementar puertas que separen sus instalaciones de la vía pública y que sean accesibles únicamente mediante llave u otorgamiento de acceso por parte de un colaborador.

3.3.7 Restricción de acceso a la información (A.8.3).

3.3.7.1 Solo se debe proporcionar a los colaboradores la información mínima indispensable para el desarrollo de sus funciones.

3.3.7.2 La información que solo deba ser usada por determinados colaboradores debe ser resguardada de manera que sea imposible su acceso accidental por parte de otras personas.

3.3.8 Inicio de sesión (A.8.15).

3.3.8.1 Todos los equipos de cómputo y celulares de la organización deben tener acceso restringido y requerir un inicio de sesión exclusivo para el usuario al que han sido asignados.

3.3.8.2 Todos los inicios de sesión deben estar protegidos por contraseñas. Quedan estrictamente prohibidos los equipos de cómputo con usuarios sin contraseña, así como las cuentas de invitado o equivalentes.

3.3.9 Autenticación segura (A.8.5).

3.3.9.1 Todas las contraseñas, siempre que el sistema asociado lo permita, deben tener al menos una mayúscula, una minúscula, un número y un caracter especial. Cuando el sistema no admita alguno de estos elementos, se deben usar tantos como sea posible.

3.3.9.2 Todas las contraseñas deben tener al menos 10 caracteres. Cuando el sistema solo admita una cantidad menor, la contraseña debe tener el máximo número aceptable de caracteres.

3.3.9.3 Las contraseñas son estrictamente personales, individuales e intransferibles, y por ningún motivo deben ser compartidas con otras personas, anotadas físicamente, mencionadas verbalmente ni registradas en archivos virtuales que pudieran ser accedidos por otra persona.

3.3.9.4 Siempre que los sistemas lo permitan, se deben establecer correos electrónicos de recuperación, preguntas de seguridad y otros controles que permitan recuperar la contraseña en caso de olvido.

3.4 Control del uso de la información.

3.4.1 Uso aceptable de la información y otros activos asociados (A.5.10).

3.4.1.1 Todos los colaboradores, contratistas y partes interesadas de la organización están obligados a usar la información y los recursos relacionados de manera ética, profesional y en línea con las políticas establecidas por la organización.

3.4.1.2 Queda estrictamente prohibido el acceso, distribución, modificación, eliminación o divulgación no autorizada de cualquier información confidencial o de uso interno.

3.4.2 Transferencia de información (A.5.14).

3.4.2.1 Cualquier transferencia de información de la organización a través de medios electrónicos se debe realizar utilizando soluciones y proveedores que cuenten, según sea apropiado, con:

3.4.2.1.1 Métodos de encriptación en tránsito, como SSL, TLS o SSH.

3.4.2.1.2 Autenticación de dos factores;

3.4.2.1.3 Cifrado de punto a punto, para el caso de mensajería instantánea.

3.4.3 Protección de registros (A.5.33).

3.4.3.1 Los registros de la organización deben ser protegidos contra uso inadecuado mediante su resguardo en repositorios restringidos.

3.4.3.2 Los registros en físico deben ser resguardados en archiveros u oficinas bajo llave, cuyo acceso deberá ser controlado de conformidad con el apartado **3.3.3** de esta política.

3.4.4 Privacidad y protección de la información de identificación personal (A.5.34).

3.4.4.1 La organización debe poner a disposición de todas sus partes interesadas los avisos de privacidad correspondientes siempre que esta obtenga de ellas cualquier dato personal.

3.4.4.2 La organización debe respetar estrictamente los requisitos establecidos por la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDP) y su Reglamento.

3.4.4.3 La Gerencia Administrativa debe conocer cuáles requisitos de la LFPDP aplican a la organización y la manera en que le aplican.

3.4.5 Escritorio y pantalla despejados (A.7.7).

3.4.5.1 Los colaboradores no deben dejar sus computadoras desatendidas más de 30 segundos sin antes bloquear la pantalla o cerrar la sesión.

3.4.5.2 Los colaboradores no deben dejar documentos físicos desatendidos encima de sus escritorios en ningún momento.

3.4.5.3 Cuando los colaboradores manden un documento a impresión, deben permanecer en la proximidad de la impresora hasta que su documento termine de imprimirse. Los colaboradores en ningún momento deben dejar documentos en impresión ni impresos desatendidos en las impresoras.

8.4.5.4 Los colaboradores no deben tomar fotografías en donde sean visibles las pantallas de sus computadoras ni las pantallas de las computadoras de otros colaboradores, a menos que sea visible únicamente el escritorio sin archivos ni carpetas.

3.4.6 Seguridad de la información para el uso de servicios en la nube (A.5.23).

3.4.6.1 Todas las plataformas en la nube deben estar protegidas mediante acceso restringido y autenticación de doble factor.

3.4.7 Eliminación de información (A.8.10).

3.4.7.1 El periodo de retención de la información debe ser determinado por cada área, observando en todo momento los requisitos legales y otros aplicables para cada tipo de documento.

3.4.7.2 Para la información que, por su relevancia para el funcionamiento y cumplimiento legal, fiscal o contable de la organización, debe tener un periodo de retención preestablecido, se deben seguir los lineamientos siguientes:

3.4.7.2.1 Se debe conservar de manera perpetua toda la información financiera (como los registros de activos fijos, inversiones permanentes, intangibles de vida indefinida, y estados financieros, entre otros), los documentos constitutivos de la organización (como el acta constitutiva, los poderes notariales, los trámites corporativos ante las secretarías de Estado, los registros de capital social y sus modificaciones, entre otros), los movimientos y registros de la estructura accionaria y los pagos de dividendos.

3.4.7.2.2 Se debe conservar por al menos 5 años toda la información de facturación, cuentas por pagar, contabilidad y fiscal.

3.4.7.2.3 Se debe conservar por al menos 5 años a partir de la terminación del contrato toda la información contractual o comercial (como contratos, anexos, convenios modificatorios y cartas compromiso, entre otros) con todos los clientes y proveedores de la organización.

3.4.7.3 Cuando un equipo sea decomisionado o reasignado, su contenido debe ser eliminado, según aplique, con un programa informático especializado para el borrado seguro de datos, que sobrescriba la información confidencial con datos aleatorios o los destruya de manera irreparable, tales como Blancco® y HDDErase® o herramientas equivalentes.

3.4.7.4 La información física de la organización debe ser eliminada, según aplique, mediante trituración o incineración.

3.4.8 Devolución de activos (A.5.11).

3.4.8.1 Los activos de información deben ser devueltos a la organización por todas las partes interesadas cuando termine su relación con la organización. Para el caso específico de los colaboradores, se deben inhabilitar todas las cuentas y accesos del usuario dado de baja.

3.4.8.2 Los activos deben ser devueltos en un plazo no mayor a 24 horas después del final de la relación y deben ser entregados completos, con los accesorios entregados originalmente y en buen estado.

4 Sobre la infraestructura de la información.

4.1 Control de las instalaciones.

4.1.1 Perímetros físicos de seguridad (A.7.1).

4.1.1.1 La organización debe establecer límites claramente definidos entre sus instalaciones y el exterior. Estos deben estar protegidos por barreras físicas como muros, puertas con cerraduras y cámaras de vigilancia.

4.1.2 Asegurar oficinas, salas e instalaciones (A.7.3).

4.1.2.1 Todas las oficinas, salas e instalaciones que contengan información sensible o sistemas críticos deben estar aseguradas con cerraduras.

4.1.2.2 Los visitantes no deben tener acceso a las instalaciones sin la debida supervisión de un colaborador.

4.1.3 Monitoreo de seguridad física (A.7.4).

4.1.3.1 La organización debe implementar un sistema de cámaras de vigilancia que monitoree en tiempo real las áreas críticas y los perímetros de las instalaciones.

4.1.3.2 Las grabaciones de las cámaras de vigilancia se deben conservar por al menos un mes.

4.2 Control del hardware.

4.2.1 Dispositivos para usuario final (A.8.1).

4.2.1.1 Los dispositivos para usuario final deben contar, como mínimo, con los siguientes controles de seguridad:

4.2.1.1.1 Sistemas operativos actualizados.

4.2.1.1.2 *Software* antivirus;

4.2.1.1.3 Contraseñas seguras de conformidad con el apartado **3.3.9** de esta política.

4.2.1.1.4 Un *firewall* activo.

4.2.1.2 Los colaboradores solo deben utilizar los equipos de cómputo y dispositivos portátiles proporcionados por la organización para el desempeño de sus labores.

4.2.1.3 Los colaboradores deben utilizar los equipos de cómputo y dispositivos portátiles proporcionados por la organización únicamente para tareas relacionadas con su trabajo. Los colaboradores no deben:

4.2.1.3.1 Descargar archivos no relacionados con su trabajo, incluyendo archivos personales.

4.2.1.3.2 Descargar ni instalar *software* no autorizado por el responsable de seguridad de la información.

4.2.1.3.3 Acceder a sitios web de *streaming*, juegos, apuestas, pornografía, deportes, entretenimiento, espectáculos y, en general, cualquier sitio que no esté relacionado con sus funciones dentro de la organización.

4.2.1.3.4 Modificar la configuración de sus equipos sin la autorización del responsable de seguridad de la información y la alta dirección.

4.2.1.3.5 Realizar cualquier cambio o instalar cualquier herramienta que permita evadir cualquier restricción del equipo.

4.2.1.4 Los colaboradores no deben acceder a redes sociales desde los equipos proporcionados por la organización, con excepción de aquellos colaboradores que las requieran para hacer publicaciones oficiales en nombre de la organización.

4.2.1.5 Aun cuando los equipos tengan *software* preinstalado que no se relacione con el trabajo de los colaboradores, los colaboradores no deben utilizarlo.

4.2.1.6 Los colaboradores deben cuidar la integridad física y técnica de los equipos que les sean asignados.

4.2.1.7 Cualquier problema técnico o necesidad de mantenimiento del equipo de cómputo debe ser reportado al responsable de seguridad de la información de inmediato. Los colaboradores no deben intentar reparaciones por cuenta propia.

4.2.1.8 Los colaboradores no deben modificar, pintar ni colocar etiquetas ni otros tipos de decoración en los dispositivos portátiles proporcionados por la organización.

4.2.2 Emplazamiento y protección de equipos (A.7.8).

4.2.2.1 Todos los equipos críticos, como servidores, deben estar ubicados en salas con acceso restringido.

4.2.2.2 La organización debe implementar medidas ambientales adecuadas, como sistemas de aire acondicionado y supresión de incendios, para proteger los equipos contra daños físicos y asegurar su funcionamiento óptimo.

4.2.3 Mantenimiento del equipo (A.7.13).

4.2.3.1 La organización debe establecer un calendario regular de mantenimiento preventivo para todos los equipos de cómputo y servidores, que incluya actualizaciones de *software*, verificaciones de *hardware* y pruebas de funcionamiento.

4.2.4 Eliminación segura o reutilización de equipos (A.7.14).

4.2.4.1 La organización debe mantener un registro de todos los equipos de la organización y su estado de validez u obsolescencia.

4.2.4.2 Cuando, por obsolescencia o descompostura, se deba eliminar un equipo, el responsable de seguridad de la información debe:

4.2.4.2.1 Realizar una copia de seguridad de toda la información.

4.2.4.2.2 Borrar de manera segura el equipo, de conformidad con lo establecido en el apartado **3.4.7.3** de esta política.

4.2.4.2.3 Desactivar las cuentas de usuario en el equipo;

4.2.4.2.4 Enviar el equipo a disposición final para su destrucción, donación o reciclaje.

4.3 Control del software.

4.3.1 Instalación de software en sistemas operativos (A.8.19).

4.3.1.1 La adquisición de licencias y *software* debe estar sujeta a la aprobación directa de la alta dirección. Aun el software gratuito debe ser aprobado por la alta dirección antes de ser instalado en cualquier equipo de la organización.

4.3.1.2 Solo el usuario asignado a un equipo debe hacer la instalación del *software* en el mismo, notificando al responsable de seguridad de la información.

4.4 Control de las redes.

4.4.1 Seguridad en redes (A.8.20).

4.4.1.1 Se debe llevar a cabo un monitoreo continuo de las redes para detectar y responder a actividades inusuales o intentos de intrusiones.

4.4.1.2 Los dispositivos de red, como *routers* y *switches*, se deben mantener actualizados con los últimos parches de seguridad y actualizaciones de *firmware* recomendados por el fabricante.

4.4.1.3 Solo los colaboradores de la organización, así como los visitantes que justificadamente lo requieran, deberán tener acceso a las redes de la organización. Queda estrictamente prohibido compartir las contraseñas de red a personas ajenas a la organización sin justificación.

4.4.1.4 Las contraseñas de todos los puntos de acceso a WiFi deben ser modificadas cuando menos una vez por mes calendario y distribuidas de manera segura a los colaboradores de la organización.

5 Sobre los eventos de la información.

5.1 Control de las amenzas.

5.1.1 Protección contra amenazas físicas y ambientales (A.7.5).

5.1.1.1 Las instalaciones de la organización deben ser protegidas de conformidad con lo establecido en plan de respuesta a emergencias.

5.1.2 Protección contra programas malignos (A.8.7).

5.1.2.1 Todos los sistemas y dispositivos de la organización deben contar con *software* antivirus o instalado y actualizado regularmente.

5.1.2.2 Se deben realizar análisis de *malware* cuando menos una vez por semana a los dispositivos de usuario final.

5.1.2.3 Los colaboradores deben informar inmediatamente al responsable de seguridad de la información de cualquier actividad sospechosa o alertas de *malware* en sus equipos.

5.1.3 Gestión de vulnerabilidades (A.8.8).

5.1.3.1 El Comité del SGI, en colaboración con los dueños y usuarios de los procesos, debe identificar las vulnerabilidades de los activos de información de la organización de acuerdo con la tabla A.11 de la norma internacional ISO/IEC 27005:2022.

5.1.4 Inteligencia de amenazas (A.5.7).

5.1.4.1 El Comité del SGI, en colaboración con los dueños y usuarios de los procesos, debe identificar las amenazas a los activos de información de la organización de acuerdo con la tabla A.10 de la norma internacional ISO/IEC 27005:2022.

5.2 Control de los incidentes.

5.2.1 Planificación y preparación de la gestión de incidentes de seguridad de la información (A.5.24).

5.2.1.1 La organización debe establecer un proceso de seguridad de la información para evaluar los eventos de seguridad de la información, determinar si se trata de incidentes y tomar las acciones adecuadas para gestionarlos.

5.2.1.2 Los eventos e incidentes de seguridad de la información deben ser utilizados para actualizar las vulnerabilidades y amenazas a la seguridad de la información, cuando sea aplicable.

5.2.2 Informes de eventos de seguridad de la información (A.6.8).

5.2.2.1 El proceso de seguridad de la información debe establecer un formato para llevar el registro de todos los eventos de seguridad de la información, sus detalles, si se trata de un incidente y las acciones realizadas para abordarlo.

5.2.3 Contacto con autoridades (A.5.5).

5.2.3.1 En caso de un ataque dirigido contra los activos de información de la organización, sean físicos o virtuales, se debe dar aviso inmediatamente a la Policía Cibernética de la Secretaría de Seguridad Pública de Puebla, a través del correo electrónico policiacibernetica@puebla.gob.mx.

5.2.4 Recolección de evidencia (A.5.28).

5.2.4.1 Para determinar si un evento de seguridad de la información constituye un incidente, el responsable de seguridad de la información debe basarse en evidencia objetiva. Tal evidencia puede incluir registros de uso de aplicativos, testimonios cruzados, grabaciones de cámaras de seguridad o cualquier otra que no dependa de supuestos o conjeturas.

5.2.5 Evaluación y decisión sobre eventos de seguridad de la información (A.5.25).

5.2.5.1 La responsabilidad de la toma de decisiones con respecto a los eventos e incidentes de seguridad de la información corresponde al responsable de seguridad de la información.

5.2.5.2 La decisión de un evento de seguridad de la información solo podrá ser si constituye o no un incidente de seguridad de la información, sin que medien otros criterios o escalas.

5.2.5.3 Para que un evento de seguridad de la información se considere un incidente de seguridad de la información, es necesario que se demuestre la pérdida de la confidencialidad, integridad o disponibilidad de algún activo de información propiedad de la organización.

5.2.6 Respuesta a incidentes de seguridad de la información (A.5.26).

5.2.6.1 Ante un incidente de seguridad de la información, el responsable de seguridad de la información, con el apoyo del Comité del SGI, debe determinar las acciones a ejecutar. Estas acciones deben lograr, según sea posibl:

5.2.6.1.1 Recuperar los activos de información expuestos, dañados, perdidos o retenidos.

5.2.6.1.2 Identificar las amenazas causantes del incidente y las vulnerabilidades explotadas de la organización.

5.2.6.1.3 Denunciar a los responsables antes las autoridades o ejecutar el proceso disciplinario al que hace referencia el apartado **3.2.7** de la presente política, cuando aplique.

5.2.6.1.4 Responder ante las partes interesadas afectadas con acciones de corrección, apoyo o compensación pertinentes, cuando aplique.

5.2.6.1.5 Actualizar la matriz de riesgos para la seguridad de la información y sus tratamientos asociados, cuando aplique.

5.2.7 Aprendizaje de los incidentes de seguridad de la información (A.5.27).

5.2.7.1 Todos los incidentes de seguridad de la información deben quedar documentados y sus registros deben ser resguardados de manera permanente por la organización.

5.2.7.2 Al responder a un incidente de seguridad de la información, se deben consultar los incidentes anteriores en busca de situaciones similares que pudieran arrojar luz sobre las mejores maneras de responder.

6 De <u>otros aspectos de seguridad de la información</u>.

6.1 Otros controles organizacionales.

6.1.1 Contacto con grupos de interés especial (A.5.6).

6.1.1.1 El responsable de seguridad de la información debe involucrarse con grupos de interés especial relacionados con la ciberseguridad para mantenerse informado sobre las mejores prácticas y amenazas emergentes. Estos grupos de interés especial pueden incluir congresos nacionales e internacionales de ciberseguridad, comunidades en línea, conferencias o materiales de difusión periódica en cualquier medio.

6.1.1.2 El responsable de seguridad de la información debe mantener evidencia de sus interacciones con estos grupos de interés especial; tal evidencia puede ser fotográfica, correos electrónicos, boletines físicos o digitales, minutas, actas o cualquier otro que se conserve como información documentada.

6.1.2 Seguridad de la información en la gestión de proyectos (A.5.8).

6.1.2.1 Al llevar a cabo proyectos, los colaboradores de la organización deben resguardar los planos y no permitir que estos sean usados o vistos por personas ajenas a la propia organización o al cliente.

6.1.2.2 Los colaboradores que participen en proyectos no deben comentar ni divulgar por ningún medio información del proyecto ni de la organización a partes externas, esto incluye revelar detalles sobre la obra a la población local.

6.1.3 Seguridad de la información en las relaciones con los proveedores (A.5.19).

6.1.3.1 Se debe informar a todos los proveedores y candidatos a proveedores de las condiciones de seguridad de la información que establece la política **PO-05 Seguridad de la información**.

6.1.3.2 Todos los proveedores de la organización deben firmar los contratos y apéndices necesarios de manera que todas sus actividades queden al amparo de las condiciones de seguridad de la información establecidas en el apartado **6.1.4**.

6.1.3.3 Para toda contratación de servicios de *software* (SaaS), se deben considerar los siguientes SLA, cuando apliquen:

6.1.3.3.1 Disponibilidad, que no podrá ser menor que el 95%.

6.1.3.3.2 Rendimiento.

6.1.3.3.3 Tiempo de respuesta de soporte técnico.

6.1.3.3.4 Cumplimiento en materia de seguridad de la información.

6.1.3.3.5 Otros que determinen los colaboradores internos de la organización.

6.1.4 Abordaje de la seguridad de la información en los acuerdos con los proveedores (A.5.20).

6.4.1.1 Cuando se contraten externamente los procesos de la organización con proveedores, los contratos celebrados con ellos deben contener:

6.1.4.1.1 Un requisito que establezca el compromiso de no utilizar la información obtenida o generada como parte de la contratación externa para beneficio propio.

6.1.4.1.2 Un requisito que establezca que solo podrán extraer de la organización la información indispensable para la realización de sus actividades y con previa autorización de las áreas usuarias.

6.1.4.1.3 Un requisito que establezca que no podrán subcontratar, sin permiso por escrito de la organización, a otras personas u organizaciones para la realización de sus actividades.

6.1.4.1.4 Un requisito que establezca que deberán notificar de cualquier incidente de seguridad de la información en un plazo no mayor a 24 horas.

6.1.4.1.5 Un requisito que establezca que deben aceptar la posibilidad de que la organización les realice verificaciones de seguridad de la información, incluyendo el acceso físico o virtual a su infraestructura.

6.1.4.1.6 Un requisito que establezca la obligación de transferir la información de manera segura, de conformidad con el apartado **3.4.2**.

6.1.4.1.7 Un requisito que establezca la obligación de eliminar la información de manera segura, de conformidad con el apartado **3.4.7** de esta política, en un plazo no mayor a un mes posterior a la terminación de sus actividades.

6.1.4.1.8 Un requisito que establezca la posibilidad de que la organización les realice auditorías de eliminación segura de la información.

6.1.5 Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC) (A.5.21).

6.1.5.1 Todas las TIC —incluyendo *hardware*, *software*, componentes de red y componentes de equipos— y los servicios relacionados con seguridad de la información deben ser adquiridos a través de proveedores que cumplan con las siguientes condiciones:

6.1.5.1.1 Estar constituidos como personas morales o personas físicas con actividades empresariales y profesionales.

6.1.5.1.2 No estar en listas negras del SAT, en caso de ser proveedores nacionales.

6.1.5.1.3 Contar con opinión de cumplimiento de obligaciones fiscales positiva por parte del SAT, en caso de ser proveedores nacionales.

6.1.5.1.4 Contar con al menos 5 años de operación.

6.1.5.1.5 Gozar de buena reputación ante la organización y sus partes interesadas.

6.1.6 Seguimiento, revisión y gestión de cambios de servicios de proveedores (A.5.22).

6.1.6.1 Se deben establecer niveles de servicio (SLA) para todos los proveedores de TIC. Estos SLA deben ser apropiados para los bienes adquiridos y el uso que la organización le dé a los mismos.

6.1.6.2 Se deben documentar y justificar todos los cambios en los SLA de los proveedores a través de minutas simples.

6.1.7 Seguridad de la información durante disrupciones (A.5.29).

6.1.7.1 En caso de robo o pérdida de equipos móviles en campo, la organización debe:

6.1.7.1.1 Activar el borrado remoto, cuando esté disponible.

6.1.7.1.2 Reportar el incidente al responsable de seguridad de la información en un plazo no mayor a 1 hora.

6.1.7.1.3 Dar de baja cualquier acceso comprometido a los sistemas corporativos.

6.1.7.1.4 Registrar el **RE-15 Evento de seguridad de la información** y categorizarlo como incidente.

6.1.7.1.5 Entregar al usuario un equipo de reemplazo.

6.1.7.2 En caso de un desastre natural que afecte las operaciones (como un terremoto), la organización debe:

6.1.7.2.1 Suspender las actividades y evacuar al personal.

6.1.7.2.2 Guardar la información y respaldarla, si el tiempo lo permite.

6.1.7.2.3 Informar la situación al Comité del SGI en un plazo máximo de 2 horas.

6.1.7.2.4 Validar la integridad de la información tras el restablecimiento de actividades.

6.1.7.3 En caso de corte prolongado de red o energía en una región, la organización debe:

6.1.7.3.1 Cambiar las operaciones administrativas al sitio alterno más cercano con conectividad, pudiendo usar también el teletrabajo.

6.1.7.3.2 Usar redes móviles con VPN para continuar transmisión, cuando menos, de información confidencial.

6.1.7.3.3 Registrar las actividades en papel o dispositivos locales cifrados si no hubiera conectividad.

6.1.7.3.4 Transferir los datos registrados una vez restablecido el servicio.

6.1.7.3.5 Informar al responsable de seguridad de la información sobre cualquier riesgo de pérdida o alteración de datos.

6.1.7.4 En caso de intrusión o acceso no autorizado a sistemas, la organización debe:

6.1.7.4.1 Bloquear el usuario, equipo o red afectada de inmediato.

6.1.7.4.2 Notificar al responsable de seguridad de la información en un plazo no mayor a 30 minutos.

6.1.7.4.3 Analizar los registros de acceso para determinar el alcance de la intrusión.

6.1.7.4.4 Cambiar las credenciales de acceso de todos los usuarios comprometidos.

6.1.7.4.5 Registrar el **RE-15 Evento de seguridad de la información** y categorizarlo como incidente.

6.1.7.5 En caso de daño físico a oficinas o instalaciones que contengan información crítica, la organización debe:

6.1.7.5.1 Resguardar documentos físicos y discos duros locales, si es seguro hacerlo.

6.1.7.5.2 Informar al Comité del SGI en un plazo máximo de 2 horas.

6.1.7.5.3 Activar el respaldo de información desde sitio alterno o nube.

6.1.7.5.4 Verificar la integridad de los respaldos y realizar restauración si es necesario.

6.1.7.5.5 Evaluar posibles filtraciones y reportar conforme a la Ley Federal de Protección de Datos Personales.

6.1.8 Preparación de las TIC para la continuidad del negocio (A.5.30).

6.1.8.1 Para asegurar que las tecnologías de información y comunicaciones estén preparadas para mantener la operación ante disrupciones, la organización debe:

6.1.8.1.1 Mantener respaldos de su información, de acuerdo con el apartado **3.1.4**.

6.1.8.1.2 Usar módems redundantes para continuar operaciones en caso de caída de la red principal.

6.1.8.1.3 Contar con equipos móviles de respaldo como laptops y celulares.

6.1.8.1.4 Asegurar que los dispositivos en campo (tabletas, laptops, celulares) sean asignados a colaboradores específicos y se encuentren protegidos por contraseña.

6.1.8.1.5 Considerar la posibilidad de operar en teletrabajo, de acuerdo con las condiciones del apartado **6.2.2**.

6.2 Otros controles de las personas.

6.2.1 Investigación de antecedentes (A.6.1).

6.2.1.1 Para reducir riesgos relacionados con el acceso a información o infraestructura crítica, la organización debe:

6.2.1.1.1 Contratar al personal con apego al procedimiento **PR-27 Contratación de personal**.

6.2.1.1.2 Solicitar carta de no antecedentes penales a todo personal de nuevo ingreso que vaya a formar parte del Comité del SGI.

6.2.1.1.3 Consultar referencias laborales previas a todo personal de nuevo ingreso que vaya a formar parte del Comité del SGI.

6.2.2 Trabajo remoto (A.6.7).

6.2.2.1 Para proteger la información cuando el personal realiza actividades fuera de oficina o en campo, la organización debe:

6.2.2.1.1 Asegurar que todo dispositivo utilizado para trabajo remoto (laptop, celular, tableta) esté protegido por contraseña o biometría.

6.2.2.1.2 Configurar el cifrado de disco completo en laptops y tablets utilizadas fuera de oficina.

6.2.2.1.3 Establecer conexión a los sistemas internos únicamente mediante VPN autorizada, cuando se acceda desde redes públicas.

6.2.2.1.4 Prohibir el uso de dispositivos personales para acceso a información de la organización, salvo autorización expresa del responsable de seguridad de la información.

6.2.2.1.5 Establecer zonas seguras para el trabajo remoto, evitando el uso de la vía pública o lugares públicos en zonas de alta criminalidad.

6.3 Otros controles físicos.

6.3.1 Trabajar en áreas seguras (A.7.6).

6.3.1.1 Para proteger la información y los activos durante la ejecución de actividades en áreas sensibles o de riesgo, la organización debe:

6.3.1.1.1 Considerar como "área segura" al sitio donde se maneje información confidencial, equipos fijos, servidores, planos técnicos y archiveros, es decir la oficina principal en Las Cruces.

6.3.1.1.2 Restringir el acceso físico a las áreas seguras únicamente al personal de la organización y visitantes necesarios.

6.3.1.1.3 Verificar la identidad del personal antes de permitir el acceso.

6.3.1.1.4 No permitir que los visitantes permanezcan sin supervisión en áreas seguras.

6.3.1.1.5 Evitar conversaciones en voz alta sobre temas técnicos, contraseñas o configuraciones en presencia de terceros o en lugares públicos.

6.3.1.1.6 Guardar bajo llave toda documentación física sensible (planos, contratos, reportes técnicos) al finalizar la jornada.

6.3.1.1.8 Denunciar inmediatamente al responsable de seguridad de la información cualquier intento de acceso no autorizado.

6.3.2 Seguridad de los activos fuera de las instalaciones (A.7.9).

6.3.2.1 Para proteger los activos de información que se utilizan fuera de las instalaciones de la organización, se debe:

6.3.2.1.1 Entregar únicamente a personal autorizado los dispositivos móviles.

6.3.2.1.2 Registrar cada entrega y devolución de activos en el vale firmado correspondiente.

6.3.2.1.3 Configurar contraseñas, cifrado de disco duro y bloqueo automático en todos los dispositivos que se usen fuera de las oficinas.

6.3.2.1.4 Evitar transportar información impresa sensible si puede enviarse por medios electrónicos.

6.3.2.1.5 No dejar equipos ni documentos visibles en vehículos, obras o alojamientos temporales sin supervisión directa.

6.3.2.1.6 Utilizar mochilas o maletines cerrados para transportar activos.

6.3.2.1.7 Reportar cualquier pérdida, robo o daño de activos al responsable de seguridad de la información en un plazo no mayor a 30 minutos.

6.3.2.1.8 No compartir activos tecnológicos (tabletas, configuradores, laptops) con personal no autorizado o sin asignación formal.

6.3.3 Medios de almacenamiento (A.7.10).

6.3.3.1 Para proteger la información contenida en medios de almacenamiento físicos o digitales, la organización debe:

6.3.3.1.1 Cifrar toda la información almacenada en discos duros externos, memorias USB, tarjetas SD y *laptops* utilizadas fuera de oficina.

6.3.3.1.2 Eliminar la información contenida en medios reutilizables antes de reasignarlos a otro usuario de acuerdo con el apartado **3.4.7**.

6.3.3.1.3 Destruir físicamente los medios de almacenamiento que estén dañados o fuera de uso, si contienen datos sensibles.

6.3.3.1.4 Evitar dejar medios portátiles sin supervisión en vehículos, obras, hoteles o áreas compartidas.

6.3.3.1.5 Reportar al responsable de seguridad de la información cualquier pérdida o robo de medios de almacenamiento de manera inmediata.

6.3.4 Utilidades de apoyo (A.7.11).

6.3.4.1 Para proteger la disponibilidad y seguridad de la información, la organización debe:

6.3.4.1.1 Verificar que todos los sitios donde operen servidores, equipos de red o estaciones de trabajo cuenten con energía eléctrica estable y regulada.

6.3.4.1.2 Instalar reguladores o no breaks (UPS) en las computadoras de escritorio y servidores.

6.3.4.1.3 Realizar pruebas mensuales de los no breaks y plantas de respaldo, asegurando su funcionamiento ante cortes eléctricos.

6.3.4.1.4 Proteger contra sobrecargas o fallas eléctricas mediante la instalación de fusibles en la acometida principal.

6.3.4.1.5 Asegurar que los equipos en campo cuenten con baterías cargadas o fuentes alternas.

6.3.5 Seguridad del cableado (A.7.12).

6.3.5.1 Para proteger el cableado que transporta información o energía en las instalaciones de la organización o de sus clientes, se debe:

6.3.5.1.1 Instalar el cableado eléctrico y de red en ductos, canaletas o charolas cerradas para evitar manipulación o daños accidentales.

6.3.5.1.2 Separar físicamente los cables de energía de los cables de datos para prevenir interferencias electromagnéticas y riesgos de incendio.

6.3.5.1.3 Fijar adecuadamente el cableado en muros, techos o zanjas para evitar cortes, tirones o vandalismo.

6.3.5.1.4 Seguir las condiciones del anexo **A** de **PR-23 Instalación y prueba de equipos** y el anexo **E** de **PR-22 Ejecución de proyectos**.

6.4 Otros controles tecnológicos.

6.4.1 Gestión de capacidad (A.8.6).

6.4.1.1 Los colaboradores deben monitorear continuamente que los sistemas que utilicen tengan la capacidad suficiente para soportar el *software* y las cargas de trabajo. En caso de detectar potenciales faltas de capacidad, como ralentización de las tareas, colapso de sistemas o fallas en el procesamiento de la información, deben reportarlas inmediatamente al responsable de seguridad de la información por medio de un correo electrónico.

6.4.1.2 El responsable de seguridad de la información debe revisar los reportes de los usuarios de la organización y determinar si se trata de faltas de capacidad genuinas o de errores en la configuración o uso de los sistemas. Aquellas faltas de capacidad confirmadas deben ser incluidas en las entradas de la revisión por la dirección para que la alta dirección pueda tomar decisiones sobre la adecuación de los recursos y, en su caso, adquirir o modificar los elementos de la infraestructura de la información.

6.4.2 Gestión de la configuración (A.8.9).

6.4.2.1 Para asegurar que las computadoras y *laptops* con sistema operen de forma segura y controlada, la organización debe:

6.4.2.1.1 Crear una cuenta de usuario personalizada con contraseña conforme con el apartado **3.3.9**.

6.4.2.1.2 Configurar la cuenta con privilegios de usuario estándar; no se deben entregar equipos con derechos de administrador local sin justificación.

6.4.2.1.3 Activar el cifrado de unidad BitLocker para proteger el disco duro en caso de pérdida o robo.

6.4.2.1.4 Configurar el bloqueo automático de pantalla tras 5 minutos de inactividad, protegido por contraseña.

6.4.2.1.5 Activar el firewall de Windows Defender® y mantenerlo activo en todo momento.

6.4.2.1.6 Activar las actualizaciones automáticas de Windows Update® al menos semanalmente.

6.4.2.1.7 Instalar antivirus y configurar análisis programados semanales (ver **5.1.2**).

6.4.2.1.8 Desinstalar cualquier *software* preinstalado que no sea necesario para la operación.

6.4.2.1.9 Configurar carpetas de trabajo (Documentos, Escritorio) para que sincronicen automáticamente con la nube o disco externo cifrado, si aplica.

6.4.2.1.10 Activar la sincronización automática con servidores de tiempo oficiales (por ejemplo, time.windows.com o ntp.org).

6.4.2.1.11 Verificar que la zona horaria esté correctamente establecida según la ubicación donde opera el equipo (por ejemplo, UTC -6 para el centro de México) y, cuando el equipo vaya a ser utilizado en campo, activar el ajuste automático de zona horaria basado en la ubicación del equipo.

6.4.2.1.12 Asegurar que dispositivos móviles, tabletas y sistemas de respaldo (como DVRs, cámaras o radios) también tengan la hora correctamente ajustada.

6.4.2.1.13 Registrar en el vale correspondiente la aplicación de la configuración anterior.

6.4.3 Enmascaramiento de datos (A.8.11).

6.4.3.1 Para evitar la exposición innecesaria de información sensible durante su uso, visualización o transferencia, la organización debe:

6.4.3.1.1 Aplicar el enmascaramiento de datos cuando se visualicen documentos que contengan información personal, financiera o técnica sensible (por ejemplo: RFC, CURP, direcciones, claves de acceso, rutas de cableado).

6.4.3.1.2 Configurar los sistemas y plantillas para mostrar solo los últimos dígitos de identificadores (por ejemplo: “***1234” para cuentas o credenciales).

6.4.3.1.3 Omitir o anonimizar información sensible al enviar capturas de pantalla, reportes, correos o evidencias operativas que serán revisadas por personal no autorizado.

6.4.3.1.4 No permitir que se impriman ni se compartan documentos completos con información confidencial sin autorización expresa del responsable de seguridad de la información.

6.4.3.1.5 Utilizar funciones de ocultamiento de datos en Excel, Word o PDF cuando se elaboren reportes para clientes o autoridades.

6.4.3.1.6 Verificar que los datos personales de empleados, clientes o proveedores no se muestren innecesariamente en sistemas compartidos o visibles en pantallas de campo.

6.4.3.1.7 Aplicar enmascaramiento durante capacitaciones, presentaciones o reuniones donde se muestren ejemplos con datos reales.

6.4.4 Prevención de fuga de datos (A.8.12).

6.1.3.1 Los colaboradores deben abstenerse de transferir, copiar, eliminar o almacenar información de la organización en dispositivos personales o medios no autorizados. El incumplimiento de este requisito debe ser investigado desde el proceso disciplinario establecido por el apartado **3.2.7** y, de demostrarse la responsabilidad del implicado, la sanción no podrá ser menor que el nivel 3.

6.1.3.2 Los colaboradores deben reportar inmediatamente cualquier intento o incidente de posible fuga de datos al responsable de seguridad de la información, por cualquier medio de contacto disponible.

6.1.3.3 El responsable de seguridad de la información puede revisar los ficheros de información y los correos electrónicos corporativos de los colaboradores en cualquier momento y sin previo aviso, esto incluye los archivos eliminados y la papelera de reciclaje o sus equivalentes en otras plataformas tecnológicas.

6.4.5 Redundancia de las instalaciones de procesamiento de información (A.8.14).

6.4.5.1 Para asegurar la disponibilidad continua de la información y los sistemas críticos ante fallas, cortes o desastres, la organización debe:

6.4.5.1.1 Utilizar servicios en la nube como respaldo de toda la información técnica, administrativa y operativa.

6.4.5.1.2 Designar como segundo punto de trabajo el domicilio particular de cada colaborador.

6.4.6 Actividades de seguimiento (A.8.16).

6.4.6.1 Para detectar, registrar y responder oportunamente a eventos que puedan afectar la seguridad de la información, la organización debe:

6.4.6.1.1 Activar los registros de eventos (logs) en computadoras, laptops y sistemas donde se almacene o procese información.

6.4.6.1.2 Verificar mensualmente los accesos y actividades en carpetas compartidas, plataformas de almacenamiento en la nube y cuentas de correo institucional.

6.4.6.1.3 Registrar en una bitácora los eventos anómalos detectados, como accesos fuera de horario, intentos de inicio de sesión fallidos, archivos modificados sin autorización, o desconexiones inesperadas.

6.4.6.1.4 Conservar los *logs* por al menos 6 meses en formato digital seguro y respaldado.

6.4.7 Sincronización de relojes (A.8.17).

6.4.7.1 Para garantizar la integridad de los registros de actividad y facilitar el análisis de eventos, la organización debe:

6.4.7.1.1 Realizar las configuraciones de los apartados **6.4.2.1.10** al **6.4.2.1.12**.

6.4.7.1.4 Prohibir el cambio manual de la hora o fecha por parte de usuarios sin autorización del responsable de seguridad de la información.

6.4.8 Uso de programas de utilidad privilegiados (A.8.18).

6.4.8.1 Para evitar el uso indebido de herramientas que puedan alterar configuraciones del sistema o comprometer la seguridad, la organización debe:

6.4.8.1.1 Identificar y autorizar únicamente los programas de utilidad que requieran privilegios administrativos, como gestores de discos, editores del registro, configuradores de red o software de diagnóstico.

6.4.8.1.2 Restringir el uso de estos programas exclusivamente al responsable de seguridad de la información o a personal autorizado por escrito.

6.4.8.1.3 Instalar estos programas únicamente desde fuentes oficiales y confiables.

6.4.8.1.4 No permitir que usuarios con cuentas estándar ejecuten herramientas con funciones elevadas (por ejemplo: cmd como administrador, regedit, gpedit.msc, software de particionado o BIOS updaters).

6.4.8.1.5 Desinstalar cualquier programa de utilidad no autorizado o que ya no sea necesario para la operación.

6.4.8.1.6 Registrar toda intervención técnica que implique el uso de herramientas privilegiadas (ejemplo: cambios en el registro, políticas del sistema, reinstalaciones).

6.4.8.1.7 Bloquear desde las políticas del sistema (gpedit) el acceso a herramientas innecesarias para los usuarios comunes.

6.4.9 Seguridad de los servicios de red (A.8.21).

6.4.9.1 Para proteger la información que circula por las redes utilizadas en oficinas, obras y campo, la organización debe:

6.4.9.1.1 Configurar contraseñas conformes con el apartado **3.3.9** en todos los dispositivos de red (módems, routers, access points).

6.4.9.1.2 Activar el cifrado WPA2 o superior en todas las redes Wi-Fi utilizadas para operaciones administrativas o técnicas.

6.4.9.1.3 Utilizar VPN para acceso remoto seguro a plataformas internas desde ubicaciones externas o móviles.

6.4.9.1.4 Mantener actualizado el firmware de los equipos de red y revisar que no tengan vulnerabilidades conocidas.

6.4.10 Segregación de redes (A.8.22).

6.4.10.1 La organización debe separar las redes de invitados o visitantes, evitando que se conecten a la misma red donde se transmiten datos operativos o administrativos.

6.4.10.2 La organización no debe permitir que personal no autorizado conecte dispositivos personales a las redes internas.

6.4.11 Requisitos de seguridad de la aplicación (A.8.26).

6.4.11.1 Para asegurar que las aplicaciones utilizadas por la organización no representen un riesgo para la información, se debe:

6.4.11.1.1 Verificar que toda aplicación utilizada para actividades laborales provenga de fuentes con buena reputación y esté actualizada.

6.4.11.1.2 Priorizar el uso de aplicaciones que incluyan funciones básicas de seguridad, como autenticación por contraseña, control de acceso y cifrado de datos.

6.4.11.1.3 No permitir la instalación de aplicaciones no autorizadas en dispositivos entregados por la organización (ver **4.2.1.3.2**).

6.4.11.1.4 Deshabilitar o restringir funciones de las aplicaciones que permitan compartir datos sin control, como exportaciones automáticas, vínculos públicos o sincronización con dispositivos personales.

6.4.11.1.5 Configurar las aplicaciones en la nube para restringir el acceso solo al personal autorizado y evitar enlaces abiertos.