**Política de Seguridad de Makita Group**

**(Revisado – 1 de abril de 2022)**

# Objetivo

Esta Política de Seguridad se aplicará a todas las Empresas del Grupo Makita para proteger los activos de información comercial e información confidencial del Grupo Makita (la "Información") y asegurar las mejores medidas posibles de Gestión de Riesgos para hacerlo.

Esta Política de Seguridad tendrá como objetivo prevenir o eliminar proactivamente las posibilidades de: (1) impacto negativo en la integridad o confianza pública en el nombre Makita; (2) pérdida financiera; (3) pérdida de posición competitiva; (4) operación comercial degradada; (5) violación de un acuerdo de protección de información de Makita con otra parte; o, (6) incumplimiento de requisitos legales o reglamentarios.

Ámbito de aplicación y definiciones

Los activos de información y la información confidencial definidos en esta Política de seguridad incluyen, entre otros: formatos de audio, visuales, escritos, magnéticos, electrónicos y ópticos para grabaciones de investigación, propiedad intelectual, desarrollo de negocios y productos, pruebas clínicas, información de entrada a AI y resultados de aprendizaje. datos de evaluación, ventas, marketing y planes de negocios, información de clientes y socios comerciales, cadena de suministro, fabricación, distribución, finanzas, recursos humanos, consultoría, asociaciones, contratos, adquisiciones, etc.

Asimismo, la Gestión de Riesgos en esta Política de Seguridad incluye medidas para identificar y prevenir amenazas al negocio, si los activos se pierden, son robados, destruidos, alterados o no están disponibles. Estos riesgos pueden ser [1] activos o intencionales (por ejemplo, causados por un empleado descontento, competidor, hacker, agencia de noticias, gobierno extranjero, etc.) o [2] de naturaleza pasiva o accidental (por ejemplo, falla de hardware o software, desastre natural, mantenimiento inadecuado, error del operador, etc.).

# Responsabilidades

Mientras que el Jefe de cada Afiliado de Makita ("Director General") puede desear nominar a uno o más empleados Afiliados responsables para administrar un programa continuo de seguridad de la información, el Director General siempre asumirá la plena responsabilidad de (1) documentar y aprobar procedimientos locales y manuales de capacitación, (2) para llevar a cabo las disposiciones de esta Política de Seguridad, y (3) establecer un programa obligatorio de educación y concientización para todos los empleados. Todas las personas deben informar cualquier violación conocida o sospechada de esta Política de Seguridad a su Director General. El Director Gerente debe investigar la causa raíz y considerar la remediación. Las violaciones de esta Política de seguridad pueden ser motivo de acción disciplinaria. Esta Política ha sido designada como Propiedad de Makita y está destinada para uso comercial interno de Makita Group. Sin embargo, puede ser proporcionada a empleados temporales, proveedores, clientes y consultores o contratistas externos cuando un Gerente ha decidido que estaría en los intereses comerciales y de seguridad de la información de Makita hacerlo, siempre que se haya ejecutado un acuerdo de confidencialidad antes de cualquier publicación de la Política.

1. Las Empresas del Grupo Makita están obligadas a cumplir o exceder esta Política de Seguridad del Grupo, y deben agregar políticas de seguridad locales para satisfacer necesidades comerciales, ambientales o legales únicas. Las políticas locales de seguridad de la información deben revisarse y actualizarse al menos una vez al año.
2. Aclaración de las personas responsables de los sistemas de información y de las personas que promueven la seguridad
   1. El Director Gerente asignará a las personas responsables de los sistemas de información y a las personas que promuevan la seguridad.
   2. El Director General asigna a las personas bajo los gerentes responsables de los sistemas de información que tienen un impacto material en los estados financieros del afiliado y reconoce oficialmente la segregación de funciones. El Director General debe informar al Departamento de Sistemas de MJ EDP de cualquier cambio en la segregación de funciones.
   3. Las personas que promuevan la seguridad deberán documentar los procedimientos y manuales de capacitación que manejan la selección, el período de administración y la disposición de los activos de información y la información confidencial definida en el frente.
   4. Las personas que promuevan la seguridad deberán aclarar con el Departamento de Sistemas de MJ EDP el método apropiado de respuesta en caso de cualquier problema o pregunta relacionada con el mantenimiento y la implementación de los sistemas.
   5. Las personas que promuevan la seguridad deberán obtener la aprobación del Director General para los procedimientos y los manuales de capacitación, y difundirlos a los empleados. Las personas que promuevan la seguridad notificarán al Comité de Seguridad de la Información de MJ[[1]](#footnote-1) sin demora y seguirán las instrucciones si encuentran una falla y problemas relacionados con los activos de información y la información confidencial.
   6. Las personas que promuevan la seguridad participarán en las reuniones mundiales celebradas periódicamente por el Equipo de Contramedidas de Seguridad Cibernética de MJ (en adelante, "CSCT"), e informarán sobre las medidas de seguridad y las actualizaciones de estado, según las instrucciones del CSCT.
3. Las Empresas del Grupo Makita prepararán un plan de negocios anual incluyendo los objetivos de TI y monitorearán el progreso según se considere necesario. Cada plan de negocios debe recibir una aprobación de la junta directiva.
4. Las Empresas del Grupo Makita llevarán a cabo la Gestión de Riesgos en los siguientes rubros:
   1. Evaluación de riesgos

El riesgo se identificará en cada empresa. Se identifican los riesgos para la continuidad general del negocio, la continuidad operativa y el cumplimiento, así como el riesgo de compromiso de los sistemas informáticos en caso de un ataque cibernético. En cuanto a los riesgos cibernéticos globales, el CSCT proporcionará orientación según sea necesario, sin embargo, para los riesgos cibernéticos locales, cada compañía individual identificará a las organizaciones que comparten inteligencia de amenazas y recopilan información de seguridad de esas organizaciones. Los riesgos incluyen no solo amenazas externas, sino también amenazas internas (como fugas de información e interrupciones del sistema debido a fraudes internos). Las características del negocio, la misión, los activos de información y la criticidad del sistema, la probabilidad de que ocurran amenazas y el impacto en el negocio se tendrán en cuenta para determinar los riesgos.

* 1. Documentación y aprobación de políticas para abordar el riesgo

Se desarrollará y documentará una política que defina cómo se monitorearán y gestionarán los riesgos en función del impacto comercial de la gravedad del riesgo, así como la forma de responder.

* 1. Implementar las medidas de gestión de riesgos

Sobre la base de la política formulada, se implementarán medidas y operaciones que disuadan el riesgo. Además, se aclararán en la documentación las posibles medidas y operaciones que pueda adoptar cada empresa.

* 1. Educación de los empleados

Las personas que promuevan la seguridad velarán por que todos los empleados de cada empresa estén informados y alertados sobre las medidas y operaciones adoptadas para disuadir los riesgos. Además, cuando se lleva a cabo capacitación relacionada con la seguridad dentro de la empresa, se deben mantener registros de capacitación.

* 1. Auditoría y autoevaluación

Los riesgos, las contramedidas y la eficacia de las operaciones se evaluarán anualmente teniendo en cuenta las últimas tendencias de amenazas, y se formulará un plan de revisión en consecuencia. Además, los resultados de la evaluación y el progreso del plan de revisión se registrarán sin falta.

* 1. Revisión de políticas

Lo anterior 1) a 5) deberá estar claramente documentado con evidencia. El Director General de cada empresa aprobará la creación, revisión o supresión de cada documento, y el documento será gestionado por el responsable del sistema y las personas que promueven la seguridad.

1. Las Empresas del Grupo Makita pasarán por controles de seguridad y obtendrán aprobación previa por escrito para las compras de hardware, software y periféricos de la sede de MJ dependiendo de los montos de acuerdo con la política y procedimientos de la compañía. Si las circunstancias hicieron imposible o poco práctica la obtención de la aprobación previa, el Director Gerente debe obtener y conservar la aprobación por escrito dentro de los 30 días posteriores a dichas compras.
2. Al desarrollar o modificar programas internos, se harán los siguientes documentos y los documentos están sujetos a los requisitos de retención de registros de Makita Group. - Formulario de solicitud realizado por el usuario - Especificaciones e informes de progreso aprobados por la persona responsable del sistema de información. Los formularios de solicitud y las especificaciones se conservarán mientras exista el sistema. Los demás documentos se conservarán durante 20 años.   
   Si las circunstancias hicieron imposible o poco práctica la obtención de la aprobación previa, el Director Gerente debe obtener y conservar la aprobación por escrito dentro de los 30 días posteriores a la finalización del desarrollo o modificación. El Director Gerente puede considerar necesario elaborar sus propios procedimientos y manuales de capacitación relativos al desarrollo o modificación de aplicaciones internas. Cuando sea necesario, se revisarán y revisarán los procedimientos y los manuales de capacitación. Los documentos revisados serán aprobados por el Director Gerente.
   1. Incluya los siguientes elementos en el formulario de solicitud: (i) número de control secuencial; (ii) el nombre y el departamento de la persona que solicita el desarrollo o modificación; iii) la fecha de solicitud; (iv) propósito del desarrollo o modificación; (v) firma de aprobación por parte del gerente del solicitante junto con la fecha de aprobación; y (vi) firma de aceptación por parte de la persona responsable del sistema de información junto con la fecha de aceptación;
   2. Se elaborarán informes de situación sobre la evolución o modificación. Los informes de situación serán examinados y aprobados por el Director Gerente.
   3. Realice una prueba de aceptación del usuario (UAT) después de completar el trabajo de desarrollo o modificación para confirmar que se han cumplido todos los requisitos del usuario.
   4. La persona responsable del sistema de información migra el software desarrollado / modificado al entorno de producción después de recibir la aprobación del usuario en función de los resultados de UAT.
3. Para proporcionar servicios informáticos estables y responder a posibles incidentes de diversas causas, la persona responsable del sistema de información debe preparar documentos tales como los diagramas de flujo del proceso informático, manuales de operaciones, registros diarios, informes de incidentes, planes de procesamiento mensuales, red de contactos de emergencia en caso de desastre, etc. y proporcionar al personal la capacitación necesaria. Además, la persona responsable del sistema de información revisará y revisará dichos documentos, según sea necesario.
4. Con respecto a la selección inicial y la renovación de proveedores de servicios externos, el Director Gerente establecerá criterios objetivos y revisará periódicamente el desempeño de los proveedores importantes:
   * + 1. Para la selección inicial, haga que varios proveedores presenten cotizaciones basadas en la naturaleza de los servicios subcontratados y los criterios de selección por escrito;
       2. Hacer que los posibles proveedores de servicios describan los servicios, recursos, precios y condiciones de pago propuestos;
       3. Según se considere necesario, realizar una investigación independiente para verificar la estabilidad y reputación del posible proveedor de servicios (consulta del banco de datos, resultados recientes de rendimiento financiero, referencias crediticias, etc.); y
       4. Para los proveedores de servicios existentes, realice una revisión periódica del desempeño por parte de varios empleados o gerentes de Makita.
       5. Cuando el proveedor de servicios desarrolle sistemas críticos (por ejemplo, sistemas que manejan servicios externos, información confidencial, información del cliente o información personal), el plan de respuesta para incidentes de seguridad como ataques cibernéticos, anomalías del sistema que afecten la prestación del servicio y fuga de información deberá articularse claramente en la cláusula contractual y acordarse por ambas partes. El plan de respuesta se refiere a 1) la persona responsable del caso, 2) la identificación de la causa (incluida la identificación de la fuente de la fuga de información), 3) la identificación del alcance del daño y el impacto (incluida la identificación del destino de la fuga de información) y 4) las medidas que deben tomarse.
       6. Además de lo anterior, defina puntos de contacto de emergencia y establezca flujos de escalamiento (incluidas las autoridades locales o reguladores relacionados, según se definan localmente). Si es probable que un incidente afecte al negocio, el Comité de Seguridad de la Información de MJ debe ser notificado sin demora, incluso si el riesgo no se ha materializado en el momento en que ocurrió el incidente.
5. Con respecto a la protección de la propiedad intelectual, los activos de información, la confidencialidad, los datos y programas de los estados financieros, la administración debe considerar los eventos pasados, así como los posibles desastres naturales futuros, ataques intencionales, accidentes (robo, destrucción de datos, inundaciones, incendios, sobretensiones, derrames químicos, terremotos, piratería, virus, etc.) en la planificación de los procedimientos de copia de seguridad de datos y los planes de recuperación de desastres. (no limitado a desastres, sino también incluyendo un plan de recuperación en caso de mal funcionamiento del sistema). Además, la gerencia debe proporcionar a sus empleados educación, capacitación y práctica adecuadas para la recuperación de fallas periódicamente (anualmente), o confirmar su efectividad y revisar el plan de recuperación en consecuencia.
6. La copia de seguridad del sistema debe realizarse diariamente en un medio desconectado de la LAN interna o en una red diferente, y la administración será responsable de conservar un registro diario. Además, la administración debe almacenar los medios de respaldo en una caja fuerte resistente al fuego y al agua con cerradura, preferiblemente lejos de la sala de computadoras y limitar el acceso a un número limitado de personal de administración.
7. Al realizar una copia de seguridad en la nube o en el centro de datos, seleccione un socio comercial confiable que haya obtenido ISO27001 o el mismo nivel de certificación. Además, asegúrese de que la comunicación de copia de seguridad utilice una línea dedicada o una línea VPN para garantizar la seguridad.
8. Identificar a las partes interesadas internas y externas relevantes y a las instituciones públicas (partes reguladoras designadas por las leyes y regulaciones locales, policía cuando esté relacionada con delitos, medios de comunicación, etc.) para escalar e informar la situación de acuerdo con el nivel de impacto de los desastres naturales, ataques intencionales, incluidos los ataques cibernéticos, y accidentes. Además, el departamento de respuesta, los respondedores y el plazo de respuesta deben estar claramente definidos y documentados.
9. Una vez que las operaciones comerciales se hayan recuperado, revise el plan con las partes relevantes para determinar si las medidas se ejecutaron como se esperaba, actualice las medidas preventivas y refleje la lección aprendida de la respuesta al incidente a los documentos existentes.
10. Monitorear el impacto del incidente tanto interna como externamente, y trabajar para restaurar la confianza y reputación de Makita Group.
11. El Director General debe evitar el acceso no autorizado a la sala de computadoras donde se encuentran los equipos de red, servidores de correo o servidores mainframe, espacio donde se almacenan los medios de software o espacio de oficina para programación. Estas áreas deben estar cerradas en todo momento y solo las personas autorizadas pueden ingresar.  
     Cuando personas no autorizadas necesitan ingresar a las áreas restringidas, el Director General debe mantener un registro del nombre de la persona junto con la fecha y la hora. Además, el personal con acceso autorizado debe verificar la identificación si es necesario y debe acompañar a los visitantes en todo momento.   
    Comer, beber o fumar en las áreas estará estrictamente prohibido. La administración debe considerar equipar las áreas con instalaciones tales como hardware redundante / tolerante a fallas, fuentes de alimentación ininterrumpida (UPS) y prevención / detección de incendios en la medida en que sea práctico.
12. En la puerta de enlace que se conecta a Internet y a redes externas, el Director General debe proporcionar software antivirus y antigusanos comercial, así como un firewall de grado comercial con una función de contramedida de ataque dirigido para evitar la entrada no autorizada. Con el fin de reducir el correo electrónico de virus y el correo electrónico no solicitado, contrate servicios de comprobación y filtrado de virus antes de recibir correo electrónico de Internet.  
     Además, el software antivirus debe ser capaz de renovar automáticamente la definición de virus y el software con análisis heurístico y notificación de informes, etc. Cuando se utilizan servicios en la nube que utilizan Internet (SaaS e IaaS de Office 365, etc.), el acceso desde la empresa es limitado y el acceso desde el exterior se limita a hardware autorizado o usuarios autorizados.
13. Para todos los software, aplicaciones y sistemas que tengan un impacto material en los estados financieros de la compañía, el Director Gerente establecerá una separación adecuada de funciones y medidas de acceso de seguridad de la siguiente manera:
    1. El gerente de un nuevo usuario del sistema (un empleado, un contratista, etc.) debe aprobar y enviar un formulario de solicitud de acceso al sistema de usuario al administrador del sistema después de considerar las descripciones de trabajo del usuario y la segregación adecuada de funciones;
    2. El administrador del sistema designado debe conceder al nuevo usuario basándose en el formulario de solicitud de acceso al sistema de usuario aprobado por el administrador del nuevo usuario.
    3. El administrador del sistema debe proporcionar al nuevo usuario un ID único y hacer que el usuario seleccione su propia contraseña única. Inicialmente, el administrador del sistema puede optar por establecer una contraseña en nombre del nuevo usuario y hacer que sea obligatorio para él / ella restablecer la contraseña en el primer inicio de sesión.  
        La contraseña tendrá una longitud mínima de ocho caracteres y deberá constar de dígitos alfabéticos y numéricos. No se permitirá a los usuarios establecer una contraseña que se pueda adivinar fácilmente y la contraseña no debe escribirse. Además, los usuarios no deben revelar la contraseña.
    4. Los usuarios normales deben cambiar la contraseña al menos cada 90 días. Los usuarios especiales, como los administradores del sistema, deben cambiar la contraseña al menos cada 45 días. La contraseña no se reutilizará durante al menos tres iteraciones o un año natural completo, lo que sea más largo.
    5. Periódicamente, se analizará si existe algún acceso no autorizado.
    6. El Director General debe dirigir un inventario físico completo de ID de usuario y autoridad de acceso al menos cada semestre . Si hay ID de usuario que no se utiliza debido a renuncias o transferencias, se eliminarán y las autoridades de acceso se revisarán si es necesario.
    7. El Director General debe asegurarse de que antes de que puedan acceder a todos los nuevos usuarios del sistema Makita sean educados con respecto a la criticidad de la gestión de la seguridad del sistema y que la educación continua sobre la seguridad del sistema sea proporcionada periódicamente (al menos una vez al año).
14. El Director General debe dirigir un inventario físico completo de todo el hardware, software y otra infraestructura del sistema al menos una vez al año. Además, se deben realizar comprobaciones, como vulnerabilidades, fin de soporte y violaciones de reglas para mantener el nivel de seguridad.
15. Seguridad de un documento confidencial: Su propósito es evitar una pérdida económica y un detrimento cuando un documento confidencial se filtra y se utiliza fraudulentamente. Debemos controlar los documentos confidenciales de la siguiente manera.
    1. Definición de documento confidencial: Documento, Datos electrónicos y medios que corresponden a la siguiente clasificación.
       1. Estrictamente confidencial: La información confidencial que influye gravemente en nuestra empresa, si se filtra. (Información que seguramente sufriremos una pérdida financiera y perderemos la confianza en la sociedad, si se filtra).
       2. Confidencial: La información confidencial que influye seriamente en nuestra empresa, si se filtra. (Información de que sufrimos una pérdida financiera o perdemos la confianza en la sociedad, si se filtra).
       3. Solo para uso interno: La información confidencial que probablemente no influye en nuestra empresa, si se filtra. (Información que probablemente no sufrimos una pérdida financiera y perdemos la confianza en la sociedad, incluso si se filtra).
    2. Normas de cumplimiento
       1. Debemos marcar "CONFIDENCIAL" al documento altamente y medio confidencial. Y debemos marcar "CONFIDENCIAL" en el documento para uso interno solo si es necesario.
       2. El trabajador que maneja confidenciales debe usarlos en el ámbito de un método predefinido y un propósito.
       3. Los documentos confidenciales se controlarán, almacenarán y destruirán adecuadamente de acuerdo con su confidencialidad.
       4. Las unidades de almacenamiento de medios seguras y encriptadas y el equipo de servicio de intercambio de archivos en preparación para un robo o pérdida son absolutamente esenciales cuando lleva cualquier documento confidencial al exterior de la oficina.
16. En caso de que factores especiales tales como requisitos comerciales, aduanas, leyes, reglamentos, etc. requieran que se modifique la Política de Seguridad, las personas que promueven la seguridad deberán obtener la aprobación del Director General y notificar inmediatamente al Presidente de Seguridad de la Información de MJ de dichos cambios y recibir su aceptación.  
     El Director General de cada afiliado de Makita es responsable de asegurar todas las disposiciones de esta Política de Seguridad y de informar al Departamento de Sistemas de MJ EDP de los resultados de cumplimiento al menos una vez al año.

1. El Equipo de Contramedidas de Seguridad Cibernética ("CSCT"), bajo la supervisión del Propietario de Seguridad, sirve como un equipo operativo para la Política de Seguridad del Grupo Makita y responde a los informes de seguridad de la información y consultas de los afiliados. [↑](#footnote-ref-1)