**Política de Seguridad del Grupo Makita**

**(Revisado – 25 de octubre de 2022)**

# Objetivo

Esta Política de Seguridad se aplicará a todas las Compañías del Grupo Makita para [[1]](#footnote-1)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 la confianza pública en el nombre de 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 los 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 comercial y de productos, pruebas clínicas, información de entrada a la IA y resultados de aprendizaje datos de evaluación, planes de ventas, marketing y negocios, información de clientes y socios comerciales, cadena de suministro, fabricación, distribución, finanzas, recursos humanos, consultoría, asociaciones, contratos, adquisiciones, etc.

Además, la Gestión de Riesgos en esta Política de Seguridad incluye medidas para identificar y prevenir amenazas al negocio, en caso de pérdida, robo, destrucción, alteración o indisponibilidad de los activos. Estos riesgos pueden ser [1] activos o intencionales (por ejemplo, causados por empleados descontentos, competidores, piratas informáticos, agencias de noticias, gobiernos extranjeros, etc.) o [2] de naturaleza pasiva o accidental (por ejemplo, fallas de hardware o software, desastres naturales, mantenimiento inadecuado, errores del operador, etc.).

# Responsabilidades

Mientras que el Jefe de cada Afiliado de Makita ("Director General") puede desear nominar a uno o más empleados responsables del Afiliado para administrar un programa continuo de seguridad de la información, el Director Gerente siempre asumirá la responsabilidad total de (1) documentar y aprobar los 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 a su Director General de cualquier violación conocida o sospechada de esta Política de Seguridad. El director general debe investigar la causa raíz y considerar la remediación. Las violaciones de esta Política de Seguridad pueden ser motivo de medidas disciplinarias. Esta Política ha sido designada como Propiedad de Makita y está destinada para uso comercial interno del Grupo Makita. Sin embargo, puede ser proporcionada a empleados temporales, proveedores, clientes y consultores o contratistas externos cuando un Gerente haya decidido que sería en los intereses comerciales y de seguridad de la información de Makita hacerlo, siempre y cuando se haya ejecutado un acuerdo de confidencialidad antes de cualquier publicación de la Política.

1. Las Compañías 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 los 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 Gerente asigna a las personas bajo los gerentes responsables de los sistemas de información que tienen impactos materiales en los estados financieros de la filial 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 se ocupen de la selección, el período de administración y la disposición de los activos de información y la información confidencial definidos en el frente.
   4. Las personas que promuevan la seguridad deberán aclarar con el Departamento de Sistemas de MJ EDP el método adecuado 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 obtendrán la aprobación del Director Gerente para los procedimientos y los manuales de capacitación y los difundirán entre los empleados. Las personas que promuevan la seguridad notificarán[[2]](#footnote-2) sin demora al Comité de Seguridad de la Información de MJ y seguirán las instrucciones, si encuentran fallas y problemas con respecto a 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 Compañías del Grupo Makita prepararán un plan de negocios anual que incluya los objetivos de TI y monitorearán el progreso según se considere necesario. Cada plan de negocios debe recibir la aprobación de la junta directiva.
4. Las Compañías del Grupo Makita llevarán a cabo la Gestión de Riesgos en el siguiente orden:
   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 ciberataque. En cuanto a los riesgos cibernéticos globales, el CSCT proporcionará orientación según sea necesario, sin embargo, para los riesgos cibernéticos locales, cada empresa individual identificará a las organizaciones que comparten inteligencia de amenazas y recopilará información de seguridad de esas organizaciones. Los riesgos incluyen no solo las amenazas externas, sino también las amenazas internas (como la fuga de información y la interrupción del sistema debido a un fraude interno). Para determinar los riesgos se tendrán en cuenta las características del negocio, la misión, los activos de información y la criticidad del sistema,[[3]](#footnote-3) la probabilidad de que se produzcan amenazas y el impacto en el negocio.

* 1. Documentación y aprobación de políticas para hacer frente a los riesgos

Se desarrollará y documentará una política que defina cómo se supervisarán y gestionarán los riesgos en función de la gravedad del riesgo, el impacto en el negocio y la forma de responder.

* 1. Implementar las medidas de gestión de riesgos

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

* 1. Educación de los empleados

Las personas que promuevan la seguridad se asegurarán de 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 una formación relacionada con la seguridad dentro de la empresa, se deben mantener registros de formación.

* 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, se registrarán sin falta los resultados de la evaluación y los avances del plan de revisión.

* 1. Revisión de Políticas.

Los puntos 1) a 5) anteriores deberán estar claramente documentados con pruebas. 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 promotoras de la seguridad.

1. Las Compañías 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 hacen imposible o impracticable 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 deben hacer los siguientes documentos y los documentos están sujetos a los requisitos de retención de registros del Grupo Makita. - 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 hacen que la obtención de la aprobación previa sea imposible o impracticable, 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 formación en relación con el desarrollo o la 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 la 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 para los avances o modificaciones. Los informes sobre la marcha de los trabajos serán revisados 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 la UAT.
3. Para proporcionar servicios informáticos estables y responder a posibles incidentes de diversas causas, la persona responsable del sistema de información preparará documentos tales como los diagramas de flujo de los procesos informáticos, los manuales de operaciones, los registros diarios, los informes de incidentes, los planes de procesamiento mensuales, la red de contactos de emergencia en caso de desastre, etc., y proporcionará al personal la formación 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 los proveedores de servicios externos, el Director Gerente establecerá criterios objetivos y revisará periódicamente el desempeño de los proveedores importantes:
   * + 1. Para la selección inicial, pida a varios proveedores que presenten cotizaciones por escrito basadas en la naturaleza de los servicios subcontratados y los criterios de selección;
       2. Hacer que los posibles proveedores de servicios describan los servicios, recursos, precios y condiciones de pago propuestos;
       3. Cuando se considere necesario, llevar a cabo una investigación independiente para verificar la estabilidad y la reputación del posible proveedor de servicios (consulta de la base de datos, resultados recientes de rendimiento financiero, referencias crediticias, etc.); y
       4. Para los proveedores de servicios existentes, realizar 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 manejen 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 se articulará claramente en la cláusula del contrato y será acordado 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 adoptarse.
       6. Además de lo anterior, defina los puntos de contacto de emergencia y establezca flujos de escalamiento (incluidas las autoridades locales o los reguladores relacionados según se defina localmente). Si es probable que un incidente afecte al negocio, se debe notificar sin demora al Comité de Seguridad de la Información de MJ, 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 gerencia debe considerar los eventos pasados, así como los posibles desastres naturales futuros, los ataques intencionales, los accidentes (robo, destrucción de datos, inundaciones, incendios, subidas de tensión, derrames químicos, terremotos, piratería, virus, etc.) en la planificación de los procedimientos de copia de seguridad de datos y los planes de recuperación ante desastres (no limitados a desastres). pero también incluyendo un plan de recuperación en caso de mal funcionamiento del sistema). Además, la gerencia debe proporcionar a sus empleados la educación, la capacitación y la práctica adecuadas para la recuperación de fallas periódicamente (anualmente), o confirmar su efectividad y revisar el plan de recuperación en consecuencia
   1. 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 mantener un registro diario. Además, la gerencia debe almacenar los medios de respaldo en una caja fuerte con cerradura resistente al fuego y al agua, preferiblemente lejos de la sala de computadoras y limitar el acceso a un número limitado de personal de administración.
   2. 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 respaldo utilice una línea dedicada o una línea VPN para garantizar la seguridad.
   3. Identificar a las partes interesadas internas y externas pertinentes y a las instituciones públicas (partes reguladoras designadas por las leyes y reglamentos 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, los ataques intencionales, incluidos los ataques cibernéticos, y los accidentes. Además, el departamento de respuesta, los respondedores y el plazo de respuesta deben estar claramente definidos y documentados.
   4. Una vez que las operaciones comerciales se hayan recuperado, revise el plan con las partes pertinentes para determinar si las medidas se ejecutaron según lo esperado, actualice las medidas preventivas y refleje la lección aprendida de la respuesta al incidente en los documentos existentes.
   5. Monitorear el impacto del incidente tanto interna como externamente, y trabajar para restaurar la confianza y reputación de Makita Group.
6. El Director Gerente debe impedir el acceso no autorizado a la sala de computadoras donde se encuentran los equipos de red, los servidores de correo o los servidores de mainframe, el espacio donde se almacenan los medios de software o el espacio de oficina para la programación. Estas áreas deben estar cerradas con llave en todo momento y solo las personas autorizadas pueden ingresar.  
   Cuando personas no autorizadas necesitan ingresar a las áreas restringidas, el Director Gerente debe mantener un registro del nombre de la persona junto con la fecha y la hora. Además, el personal con acceso autorizado deberá verificar la identificación en caso de ser necesario y deberá acompañar a los visitantes en todo momento.  
   Queda terminantemente prohibido comer, beber o fumar en las zonas. La gerencia debe considerar equipar las áreas con instalaciones tales como hardware redundante/tolerante a fallas, sistemas de alimentación ininterrumpida (UPS) y prevención/detección de incendios en la medida en que sea práctico.
7. En la puerta de enlace que se conecta a Internet y a redes externas, el Director General debe proporcionar software antivirus y antigusanos comerciales, así como un firewall de grado comercial con una función de contramedidas 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 verificación 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 al hardware autorizado o a los usuarios autorizados.
8. Para todo el software, aplicaciones y sistemas que procesan datos de información críticos para el negocio de Makita, el Director General deberá establecer una segregación apropiada de tareas y medidas de seguridad de acceso de la siguiente manera:
   1. El administrador 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 en función del formulario de solicitud de acceso al sistema del 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 al menos ocho caracteres y deberá constar de dígitos alfabéticos y numéricos. Los usuarios no podrán establecer una contraseña que pueda adivinarse fácilmente y la contraseña no deberá anotarse. Además, los usuarios no deben revelar la contraseña.
   4. Los usuarios habituales 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 calendario completo, lo que sea más largo.
   5. Periódicamente, se analizará si existe algún acceso no autorizado.
   6. El Director Gerente debe dirigir un inventario físico completo de la identificación de usuario y la autoridad de acceso al menos cada dos meses . En caso de que existan identificadores de usuario que no se utilicen debido a renuncias o transferencias, se eliminarán y se revisarán las autoridades de acceso 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 (por lo menos una vez al año).
9. Las Compañías del Grupo Makita recopilarán y almacenarán registros de sistemas críticos (por ejemplo, sistemas que proveen servicios externamente, almacenan información confidencial, información financiera como pagos a proveedores/vendedores, información de clientes, o información personal, sistemas de misión crítica).
   * + 1. Definir los sistemas para los que se van a recopilar los registros
          1. Sobre la base de la evaluación del riesgo, la criticidad del sistema se clasificará en "Alta", "Media" o "Baja".
       2. Recopilación de registros

Como medida de ciberseguridad, se obtendrán registros (hora, origen y destino, detalles del evento, etc.) que muestren las actividades del usuario y del sistema para que puedan ser analizados y rastreados en caso de ciberataque.

* + - * 1. Los cuatro tipos de registros que figuran a continuación se recopilarán y almacenarán como elementos básicos.
    - Registros de acceso [[4]](#footnote-4)(Fuente: sistemas aplicables)
    - Registros de autenticación (Origen: servidor de autenticación)
    - Registros de comunicación de redes externas (Fuente: DNS, Servidor proxy, Firewall)
    - Registros de eventos del sistema (Fuente: Servidores o software de seguridad aplicables)
      * 1. Para los sistemas cuya criticidad se clasifica como "alta", además de los registros anteriores, se requiere la recopilación de registros como registros de operaciones de usuario, registros de errores, registros relacionados con cambios de configuración del sistema, etc.
        2. Asegúrese de que los relojes de los sistemas estén sincronizados para que se pueda realizar un análisis de correlación durante el análisis de registros.
        3. Las funciones de registro y la información de registro deben protegerse contra la manipulación o el acceso no autorizado. Se deben tomar medidas para almacenar los registros en un medio separado del servidor desde el que se registran, o en un servidor con diferentes credenciales, cintas o registros cifrados, etc.
      1. Almacenamiento de registros

Sobre la base de la criticidad del sistema definida en a), los registros se almacenarán durante los siguientes períodos de tiempo.

|  |  |  |  |
| --- | --- | --- | --- |
| Criticidad del sistema | Bajo | Medio | Alto |
| Período de almacenamiento | Más de 2 semanas | Más de  6 meses | Más de  18 meses |
| Rotación de troncos[[5]](#footnote-5) | Opcional | Opcional | Cada 24h |
| Comprobación de la integridad del archivo de registro | Opcional | Obligatorio | Obligatorio |

* + - * 1. Asigne la capacidad de almacenamiento adecuada para los registros y almacene los registros en consecuencia.
        2. Realice comprobaciones de integridad, compruebe periódicamente si los registros se almacenan correctamente (sin errores de almacenamiento, sin archivos de registro vacíos) e informe de los registros a la persona responsable de los sistemas de información. En caso de emergencia, los registros se pondrán a disposición del CSCT y del Departamento de Sistemas de MJ EDP.
      1. Registros de supervisión

Supervise las alertas sobre errores de eventos (finalización anormal del proceso), errores de acceso (error de autenticación), etc., además de errores en la recopilación de registros. Si se encontró alguna alerta, compruebe los registros y compruebe si se ha producido un acceso no autorizado o la divulgación de información, o si se trata de un falso positivo. Si no está claro qué acción se debe tomar en respuesta al contenido de una alerta para cada software de seguridad, etc., consulte con el proveedor del producto o consulte con el CSCT.

Las personas encargadas de recopilar y administrar los registros se limitarán a un mínimo de usuarios privilegiados.

1. 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.
2. Aseguramiento de seguridad para un documento confidencial: Su finalidad es evitar una pérdida económica y un perjuicio cuando un documento confidencial se filtra y se utiliza de forma fraudulenta. Debemos controlar los documentos confidenciales de la siguiente manera.
   1. Definición de documento confidencial: Documento, Datos electrónicos y Soportes que correspondan a la siguiente clasificación.
      1. Estrictamente Confidencial: Es la información confidencial que influye gravemente en nuestra empresa, en caso de que se filtre. (Información de 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, en caso de que se filtre. (Información de que sufrimos una pérdida económica o perdemos la confianza en la sociedad, si se filtra).
      3. Solo para uso interno: La información confidencial que probablemente no influya en nuestra empresa, si se filtra. (Información de que probablemente no suframos una pérdida financiera y perdamos la confianza en la sociedad, incluso si se filtra).
   2. Reglas 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 se lleva cualquier documento confidencial al exterior de la oficina.
3. En caso de que factores especiales como requisitos comerciales, costumbres, leyes, reglamentos, etc. requieran la modificación de la Política de Seguridad, las personas que promuevan la seguridad deberán obtener la aprobación del Director Gerente y notificar inmediatamente al Presidente de Seguridad de la Información de MJ de dichos cambios y recibir su aceptación.  
   El Director General de cada filial 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.

Componentes de la política

Como componentes de esta Política de Seguridad del Grupo Makita, se formulan políticas por dominios de seguridad. Para conocer los controles y medidas específicos para cada área, consulte los siguientes documentos.

* 1. Gestión de accesos

Controles y directrices para la gestión de accesos en función de los niveles de riesgo.

* 1. Protección de datos

Controles para garantizar la seguridad de documentos y datos confidenciales.

* 1. Gestión de endpoints

Controles para garantizar la seguridad de los dispositivos que procesan datos confidenciales. Esta política se refiere a los dispositivos utilizados para las comunicaciones de TI y no incluye los equipos utilizados para el control de las instalaciones.

* 1. Seguridad de las aplicaciones

Controles para garantizar la seguridad en el ciclo de vida de desarrollo (DLC) al desarrollar aplicaciones.

* 1. Seguridad en la nube

Controles y puntos de control cuando se utilizan servicios en la nube.

1. Como Makita Japón tiene una Política de Seguridad de la Información detallada, Makita Japón cumplirá con la política detallada. [↑](#footnote-ref-1)
2. 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 a las consultas de los afiliados. [↑](#footnote-ref-2)
3. Para clarificar el nivel de impacto en el negocio como todo el Grupo Makita, la "Criticidad del Sistema" se decidirá utilizando los criterios estandarizados a nivel mundial. (Utilice "Sistema Hoja de evaluación de criticidad.xlsx".) Si hay una brecha en el resultado entre lo global y lo local, tendrá prioridad la mayor criticidad del sistema. [↑](#footnote-ref-3)
4. Los elementos que se recopilarán son el ID de usuario, la dirección IP, el sistema de acceso y la hora de acceso. [↑](#footnote-ref-4)
5. Los registros se rotarán de formas específicas para poder encontrarlos y analizarlos. Si los registros se registran continuamente en el mismo archivo, el tamaño del archivo aumentará, ocupará espacio y dificultará la búsqueda de la información necesaria en caso de emergencia. [↑](#footnote-ref-5)