Declaración de política sobre seguridad de la información

Mensaje de Forrest Smith, Director Ejecutivo de Seguridad de la Información de Ingram Micro:

"En Ingram Micro, reconocemos que la información es el alma de la empresa. Es la manera de comunicarnos y realizar negocios con usted, con nuestros valiosos clientes y con los socios proveedores.

Tratamos la información y los recursos de la empresa con respeto y los protegemos de su uso indebido, ya sea intencional o accidental. Hemos establecido una Política sobre Seguridad de la Información y medimos su éxito a través de la certificación estándar de la industria".

El objetivo de este documento consiste en demostrar que nuestro programa de Seguridad de la Información es operado de manera coherente con los estándares de la industria.

Capacitación sobre Seguridad de la Información

Cada año, se brinda formación a todos los usuarios de tecnología de la información sobre temas como seguridad de la información, protección de datos, cumplimiento normativo y concienciación.

Seguridad de la Información y Protección de la Privacidad

Mantenemos al tanto y capacitamos a todos nuestros asociados sobre las siguientes políticas relacionadas con la protección de la información y los recursos de datos:

Recursos de Información	• Todos los recursos de la Compañía (incluidas sus redes) son proporcionados con fines de uso comercial. • Definimos usos aceptables de nuestros datos y recursos.
Clasificación y Protección de la Información	• La información de la Compañía debe ser clasificada correctamente, ser protegida y distribuida de manera segura. • Marcamos los documentos con sus clasificaciones de datos: Altamente confidencial, Confidencial y Público. • Protegemos la información en base a su clasificación. • Preservamos los datos según nuestros cronogramas de retención de registros.
Autorización sobre los Datos y Recursos de la Compañía y Acceso a Ellos	• Los Asociados deberán tener los privilegios mínimos necesarios para realizar sus funciones laborales. • Inhabilitamos/eliminamos el acceso o los ID cuando ya no son necesarios. • Periódicamente, revisamos el acceso a fin de garantizar que los asociados tengan el nivel apropiado de acceso a sus posiciones y responsabilidades.
Acceso Especial y Privilegiado	• El acceso especial y privilegiado debe estar justificado, relacionarse con el rol del solicitante y tener los menores privilegios posibles necesarios para desarrollar sus funciones laborales.

Gestión y Denuncia de Incidentes de Seguridad	• El equipo de Seguridad de la Información es responsable de investigar los eventos e incidentes de seguridad de la información.
Supervisión	• Los usuarios de los servicios de tecnología de Ingram Micro están sujetos a la supervisión de cualquier recurso, sistema o red de Ingram Micro.
Viajes con Recursos o con Información de la Compañía	• Cumplimos con las leyes de control de exportaciones cuando los asociados viajan entre países.
Proteger los Recursos de la Compañía contra el Robo	• Los recursos de la Compañía deben ser protegidos contra el robo. • El robo o la pérdida de recursos de la compañía deben ser denunciados e investigados.
Actividades Delictivas	• Las actividades delictivas, relacionadas con el robo de datos o con la tecnología de la información, son investigadas por el equipo de seguridad de la información. • Cooperamos y colaboramos con el cumplimiento de la ley en las investigaciones de delitos.
Solicitudes de Cumplimiento de la Ley	• Las Solicitudes de Cumplimiento de la Ley están bajo el control del departamento legal.
Material Ofensivo	• Los Asociados no deberán usar los recursos de la Compañía ni su tiempo para acceder a material ofensivo, ni distribuirlo.
Capacitación sobre Confidencialidad y Seguridad Cibernética	• Se requiere a todos los usuarios que completen la capacitación asignada para la fecha límite requerida.
Adquisición de Tecnología	• En el proceso de adquisición de tecnología está involucrada la seguridad de la información.
Gestión de Contraseñas	• Los requerimientos de contraseñas son definidos y ejecutados en toda la organización. • Se prohíbe a los usuarios compartir sus contraseñas con otros.
Privacidad	• Solo deberán almacenarse los Datos Personales en aplicaciones aprobadas por la Compañía. • Los Datos Personales solo deberán ser recopilados y procesados con fines comerciales legales y legítimos. • La compartición de datos personales con terceros requiere de la aprobación del Director Ejecutivo de Seguridad de la Información.
Solicitudes de Auditorías y Cumplimiento de Reglamentaciones	• Todos los usuarios deben cumplir con las leyes, reglamentaciones y programas de cumplimiento respecto del uso de datos, redes y sistemas de computadoras.
Tratamiento de los Datos de Tarjetas de Crédito	• Todos los usuarios deberán cumplir con los estándares de la Industria de Tarjetas de Pago ("PCI") para procesar, almacenar y transmitir datos de tarjetas de crédito.
Escritorio Limpio	• Todos los Asociados son responsables de asegurarse de que los recursos de Ingram Micro y su información privada no queden desprotegidos cuando no están en uso en los espacios de trabajo personal y público.
Traiga su Propio Dispositivo (BYOD)	• Los dispositivos móviles personales aprobados podrán ser usados para acceder a las herramientas de colaboración de la Compañía.
Investigaciones a la Política de Seguridad de la Información	• Las Infracciones a la política de Seguridad de la Información son investigadas por el equipo de Investigaciones de Seguridad.

Grabaciones de Audio y Video	• Aunque la grabación de audio o video de las actividades comerciales está prohibida, algunos empleados están autorizados a grabar las reuniones de Teams, pero solo con el consentimiento expreso de todos los asistentes.

Gestión de la Tecnología Reguladora de las Políticas

Mantenemos al tanto y capacitamos a todo nuestro personal de TI sobre las siguientes políticas relacionadas con la protección de la información y los recursos de datos:

Infraestructura	• Ingram Micro ha adoptado la Infraestructura de Seguridad Cibernética (CSF, en inglés) NIST como su infraestructura oficial en dicha seguridad.
Cumplimiento	
Programas de Cumplimiento	• Ingram Micro implementa controles para cumplir con los siguientes programas de cumplimiento: Industria de tarjetas de pago (PCI), Estándar de seguridad de datos (DSS), Cifrado de punto a punto de PCI (P2PE), Número de identificación personal (PIN) de PCI, Ley Sarbanes Oxley (SOX) e ISO 27001:2013.
Controles Generales de TI y Propietarios de Controles	• Deberá identificarse un propietario por cada requerimiento o control del programa de cumplimiento.
Riesgos, Deficiencias y Planes de Remediación	• Deberá asignarse a un ejecutivo y a un propietario de control a cada riesgo, deficiencia y plan de remediación.
Auditoría y Acceso	• Una vez aprobado por el Director Ejecutivo de Seguridad de la Información, se le brindará acceso a todo asociado de operaciones de infraestructura (o personal contratado) o seguridad de la información (incluyendo, en los casos correspondientes, acceso administrativo) a todo recurso de Ingram Micro a los fines de cumplir con la presente política, sus deberes y responsabilidades o con el fin de realizar una auditoría.
Identificación	
Inventario y Gestión de Activos (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05)	• Todos los recursos de la compañía (dispositivos físicos, software, software como servicio, infraestructura en la nube, aplicaciones y herramientas de desarrollo interno, etcétera) deberán ser inventariados.
Roles y Responsabilidades (GV.RR-02, GV.SC-02)	• Ingram Micro ha definido claramente los roles y las responsabilidades relacionados con la seguridad cibernética y la privacidad.
Continuidad Comercial y Recuperación ante Desastres (GV.OC-05, GV.OC-04)	• El Director de Operaciones de Seguridad, en coordinación con los líderes ejecutivos, deberá establecer un plan de continuidad comercial.
Comunicación (GV.PO-01)	• Las políticas sobre seguridad de la información deberán ser comunicadas anualmente a todos los asociados como parte de la capacitación anual obligatoria.
Revisión de Políticas (GV.OC-03)	• La política sobre seguridad de la información deberá ser revisada anualmente por el Director Ejecutivo de Seguridad de la Información.
Gestión de Riesgos (GV.RM-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-01, GV.RM-02)	• Todos los riesgos relacionados con la TI deberán ser denunciados al equipo de Seguridad de la Información.

	• Todos los riesgos deberán ser analizados en cuanto a su severidad y tomarse medidas al respecto (mitigarlos, aceptarlos, evitarlos, transferirlos o una combinación de ellos).
Vulnerabilidades de Activos (ID.RA-01)	• Las vulnerabilidades son remediadas según los estándares internos y de la industria.
Eventos, Amenazas e Incidentes de Seguridad de la Información (ID.RA-03)	• Todos los eventos de seguridad de la información, amenazas e incidentes son identificados, documentados y resueltos usando los procedimientos operativos estándares aprobados.
Gestión de Riesgos de la Cadena de Suministro (GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-08)	• Deberá negociarse un acuerdo de seguridad de la información con un tercero cuando Ingram Micro le procure tecnología, cuando intercambie datos de Ingram Micro o cuando se beneficie de la adquisición o intercambio de datos.
Protección	
Gestión de Riesgos de la Cadena de Suministro (GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-08)	• Se cumplen procedimientos operativos estándares en cuanto a aprovisionamiento, desabastecimiento, realización de revisiones de acceso del usuario, otorgamiento de autorizaciones y ejecución de restablecimiento de contraseñas.
Acceso Físico (PR.AA-06)	• El Acceso Físico a los recursos del servidor de Ingram Micro deberá restringirse a aquellos con un motivo justificable de acceso al área controlada.
Acceso Remoto (PR.AA-03, PR.AA-05, PR.IR-01)	• El acceso por consola deberá ser accesible solo vía las redes internas y nunca quedar expuesto al Internet. • Todo acceso remoto deberá hacerse a través de VPN, VDI o Citrix corporativos autorizados por InfoSec y con soporte de TI. • Todo acceso remoto requiere de una autenticación multifactorial.
Red (PR.IR-01, PR.IR-02)	• Ingram Micro utiliza la segmentación de la red si implementa nuevos recursos.
Autenticación (PR.AA-03)	• Todas las aplicaciones nuevas (y las que tengan alguna modificación importante) deberán usar almacenamientos de identidades centralizados para la autenticación.
Capacitación (PR.AT-01, PR.AT-02, GV.RR-01)	• Todos los usuarios deberán participar en capacitaciones anuales de información, cumplimiento, privacidad y seguridad de la información, y realizar dichas capacitaciones para la fecha límite establecida por el Director Ejecutivo de Seguridad de la Información.
Los Datos se Protegen, se Archivan Correctamente y se Eliminan (PR.DS-01, PR.DS-02, ID.AM-07, ID.AM-08, PR.PS-03)	• Todos los datos de Ingram Micro son categorizados como Altamente Confidenciales, Confidenciales o Públicos. • Los datos son protegidos y gestionados en base a su clasificación. • Cuando ya no se necesiten, todos los datos se archivan y se retirar de línea. • Los datos son destruidos conforme al cronograma de retención de registros.
Cifrado (PR.DS-02, PR.DS-01)	• Los datos Altamente Confidenciales son cifrados en reposo y en tránsito.
Verificación de Integridad (PR.DS-01, ID.RA-09)	• Los procedimientos operativos estándares incorporan un proceso de revisión de la integridad del software, firmware y hardware.
Entornos (PR.IR-01)	• El entorno de producción deberá estar separado por completo de los entornos de prueba.

	• Los datos de producción no deberán ser usados en entornos no productivos.
Trabajos por Lotes (PR.PS-04, PR.AA-05)	• Deberá haber un proceso de supervisión del procesamiento de los trabajos por lotes, las interfaces del sistema y las transmisiones de datos.
Configuración Base y Endurecida (PR.PS-04, PR.AA-05)	• Todos los recursos implementan una guía de configuración protegida y de línea de base desarrollada por el departamento de Seguridad de la Información.
Control de Cambios (ID.RA-07, ID.AM-08)	• Todos los cambios siguen el procedimiento operativo estándar de control de cambios publicado por el equipo de Gestión de Servicios de TI.
Copia de Seguridad de Datos y Recuperación ante Desastres (PR.DS-11)	• Todos los datos tienen una copia de seguridad con las herramientas aprobadas por el VP de Operaciones Globales de Infraestructura.
Plan de Respuesta ante Incidentes de Seguridad y Plan de Recuperación ante Desastres (ID.IM-04, ID.IM-02)	• El Equipo de Seguridad de la Información gestiona un plan de respuesta ante incidentes.
Acceso al Equipo o a los Datos de los Usuarios (ID.AM-08, PR.PS-02, PR.PS-03)	• El acceso a los datos de los usuarios queda restringido a los propósitos permitidos por el Director Ejecutivo de Seguridad de la Información.
Tecnología Protectora	• La tecnología protectora estándar de la industria es implementada en profundidad para proteger los recursos y los datos.
Detección	
Anomalías, Eventos y Monitoreo Continuo de Seguridad (ID.AM-03, DE.AE-02, DE.AE-03, DE.AE-08, DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, ID.RA-01, DE.AE-06)	• El departamento de Seguridad de la Información recopila y analiza los registros de manera central en cuanto a comportamientos anómalos (evento de seguridad). • Se analizan los eventos de seguridad y se los correlaciona (desde múltiples fuentes); y se determina el impacto potencial.
Procesos de Detección (GV.RR-02, ID.IM-03)	• El Centro de Operaciones de Seguridad (SOC) es responsable de detectar y reaccionar ante las anomalías, los eventos y alertas de monitoreo continuo de seguridad.
Respuestas	
Plan de Respuesta a Incidentes de Seguridad (SIRP) (ID.IM-04, ID.IM-02, RS.MA-01)	• Se establecen, gestionan y prueban los planes de respuesta y recuperación ante incidentes y desastres.
Planificación de Respuestas (RS.MA-01)	• Contamos con un equipo capacitado y un proceso establecido de respuesta ante incidentes de la seguridad.
Comunicaciones (PR.AT-01, RS.CO-02, RS.CO-03, RS.MA-01)	• Se han establecido protocolos de comunicación y se los integra al plan de respuesta a incidentes.
Investigación (RS.MA-02, RS.MA-04, RS.AN-06, RS.AN-07, RS.MA-03, ID.RA-08)	• El plan de respuesta ante incidentes incluye una tarea de investigación con el fin de determinar la causa raíz y, en los casos posibles, su atribución.
Contención y Remediación (RS.MI-01, RS.MI-02, ID.RA-06)	• Como parte del plan de respuesta ante incidentes: (a) se implementa un plan de acción para reducir y mitigar el riesgo dentro de las 24 horas; (b) se ejecuta un plan de contención lo más rápido posible para contener el riesgo y (c) se ejecuta un plan de remediación para restaurar los servicios.

Recuperación	
Planificación de Recuperación (RC.RP-01, ID.IM-02, RS.MA-01)	• Deberán ejecutarse y mantenerse procesos y procedimientos de recuperación para garantizar la restauración de los sistemas o los recursos afectados por los incidentes de seguridad cibernética.
Mejoras (ID.IM-03)	• Deberán mejorarse las actividades y las medidas de respuesta mediante la incorporación de las lecciones aprendidas de los eventos o incidentes actuales y anteriores de seguridad.
Desarrollo, Seguridad y Operaciones	
Desarrollo, Seguridad y Operaciones (ID.AM-08)	• Todos los proyectos de TI siguen un ciclo de desarrollo de software y de gestión estándar del proyecto.
Capacitación en Seguridad	• Anualmente, se ofrece a los desarrolladores una capacitación especializada.
Documentación de Seguridad Requerida	• Para todo proyecto nuevo de desarrollo, se requiere de un conjunto estándar de entregas de seguridad. Se las revisa y aprueba en la oficina del Director Ejecutivo de Seguridad de la Información.
Herramientas y Bibliotecas de Código Abierto	• Cuando se emplean herramientas de código abierto, se implementa un plan completo que abarca pruebas de penetración y análisis de la estructura del software.
Technology Security Requirements (PR.AA-03)	• Para los proyectos nuevos, deben implementarse controles estándares y contramedidas, según lo descripto en la política.
Revisión de Seguridad Final	• El Director Ejecutivo de Seguridad de la Información debe aprobar cualquier software nuevo o modificado significativamente antes de que entre en funcionamiento y esté disponible para los usuarios.
Fusiones y Adquisiciones	
Diligencia Debida	• El equipo de seguridad cibernética realiza una diligencia debida sobre toda potencial adquisición y desarrolla un plan potencial de integración (incluyendo la remediación de las lagunas en la política).
Integración	• Se ejecuta un plan de integración estándar en todas las adquisiciones.

Consecuencias del Incumplimiento y Excepciones

Evasión de los Controles de Seguridad	• Evadir o intentar evadir los controles de seguridad de la información derivará en la desvinculación del empleo.
Infracciones y Medidas Correctivas	• Las infracciones a la política de la Compañía derivarán en medidas tomadas por el área de RR. HH., hasta e incluyendo la desvinculación. Al momento de ser notificados sobre su disconformidad, se les requiere a los Usuarios tomar medidas inmediatas para corregir dicha disconformidad.
Solicitudes de Excepción a la Política	• Solo el Responsable de Seguridad de la Información está autorizado para otorgar una excepción a la política de Seguridad de la Información.

Seguridad de la Información de Contacto

Operaciones de Seguridad de la Información
infosec@ingrammicro.com

Oficina del Director Ejecutivo de Seguridad de la Información
ciso@ingrammicro.com