Política de Seguridad en los Dispositivos de Usuario Final

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Diego González	12-04-2024	Creación del documento	INNOVATE DC	Público
2.0	Diego González	02-07-2024	Remediación de la supervisión de equipos de proveedores	INNOVATE DC	Público
2.1	Diego González	21-08-2025	Correcciones y aclaraciones sobre obligatoriedad	Diego A. González	Público

RANKMI

Chile

Responsable de actualizar y revisar el documento

Head of Security

Introducción

La Administración de Seguridad en Dispositivos de Usuario Final se refiere a la aplicación de requisitos de seguridad para garantizar la protección y gestión adecuada de los dispositivos utilizados por los usuarios finales. Establece medidas para salvaguardar la confidencialidad, integridad y disponibilidad de los dispositivos, asegurando su configuración segura, actualizaciones regulares y control de acceso.

Modelo de negocio

Rankmi es una empresa que brinda un software como servicio (SaaS) enfocado a la Gestión del Talento Humano a través de módulos cómo Beneficios, Payroll, Evaluaciones de Desempeño, Clima Laboral, Reconocimiento, LMS, ATS, Genius (módulo de IA), Hub Social, entre otros, dirigidos especialmente a medianas y grandes empresas de Latinoamérica.

Propósito del documento

Este documento tiene como objetivo establecer las directivas generales y máximas respecto de las medidas de seguridad en los dispositivos de los usuarios que se deben adoptar en Rankmi.

Alcance de la Política

Esta política es de cumplimiento obligatorio para el personal que participan en los servicios destinados al sistema de seguridad de la Información en los dispositivos de Rankmi.

Política

El responsable de administración de dispositivos debe gestionar la seguridad de los dispositivos de los empleados que tienen acceso a información confidencial y a los sistemas críticos de la empresa. Para ello debe realizar actividades de control y supervisión dentro de los diferentes escenarios de trabajo.

Sección 1:Trabajo remoto

- Supervisar que los dispositivos cuenten con controles de acceso con factores de autenticación fuerte en función de la clasificación información o sistemas que serán accedidos para evitar el ingreso de personas ajenas como familiares o extraños en áreas públicas.

- Monitorear las redes domiciliarias y redes públicas, a las que los dispositivos tienen acceso.

- Configurar en los dispositivos el uso de firewalls, protección contra malware y cifrado de disco (en Mac, por ejemplo, Filevault activo).

- Supervisar (a través de muestras aleatorias en los usuarios) que las personas no mantengan información confidencial almacenada en sus dispositivos sino que sean subidas a las plataformas y medios de almacenamiento virtual que brinda la empresa. Esta medida servirá también como respaldo para la continuidad del negocio.

- Supervisar que los propietarios de los activos usen una definición del trabajo permitido, la clasificación

de la información que puede ser mantenida y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder.

- Proveer soporte y mantenimiento para el hardware y software de los dispositivos de los usuarios que guardan o procesan información

- Realizar sesiones de auditoría y seguimiento de la seguridad, sobre los computadores a través de muestras o herramientas automatizadas.

- Realizar la revocación de autorización y derechos de acceso y supervisar la devolución de equipos cuando se dan por terminadas las actividades del trabajo a distancia.

Sección 2: Seguridad de los activos fuera de las instalaciones

- Cuando sea necesario y práctico, exigir autorización para retirar equipos y medios de las instalaciones de la organización y mantener un registro de dichas retiradas a fin de mantener una pista de auditoría. En este caso, cuando se transfiera equipo fuera de las instalaciones entre diferentes personas o partes interesadas, llevar un registro que defina la cadena de custodia del equipo, incluyendo al menos los nombres y organizaciones de los responsables del equipo. La información que no necesita ser transferida con el activo debería eliminarse de forma segura antes de la transferencia.

- En los casos que sea posible realizar la implementación de rastreo de ubicación y capacidad para borrar dispositivos de forma remota.

Sección 3: Medios de almacenamiento físico (media, memorias o papel)

En los casos en los que sea prohibido por los propietarios de los activos o los jefes de áreas, restringir el acceso a medios de almacenamiento extraíbles en los dispositivos.

Sección 4: Dispositivos de punto final de usuario

- Controlar, supervisar y configurar la restricción de la instalación de software no confiable.
- Supervisar que esté habilitado el control de acceso a dispositivos
- Supervisar el cifrado del dispositivo de almacenamiento;
- protección contra malware;
- En caso de robo o pérdida, en la medida de lo posible, configurar la desactivación, borrado o bloqueo remoto del dispositivo.
- Supervisar que realizan copias de seguridad en los sistemas documentales provistos por la empresa.
- Configurar restricciones de uso de servicios web y aplicaciones web
- En el caso de personal que tenga acceso a información confidencial y crítica para el negocio, realizar un análisis periódico del comportamiento del usuario final.

Sección 5: Protección contra malware

- Instalar y actualizar regularmente el software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónico.
- Este software debe escanear cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso.
- Este software debe escanear páginas web en busca de malware cuando se accede a ellas.

Sección 6: Uso de programas de utilidad privilegiados

Limitar el uso de programas de utilidad al número mínimo necesario para usuarios autorizados.

Sección 7: Filtrado web

Identificar y bloquear los sitios web a los que el personal debería o no tener acceso. ● Sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas. ● Sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing). ● Sitio web malicioso adquirido por inteligencia de amenazas.

Aprobación y Revisión

Los miembros del Comité Directivo que aprueban la versión vigente de la presente política es:

Nombre	Cargo	Fecha de Revisión
Diego A. González	CISO	12/04/2024
Felipe Mundaca	CTO	12/04/2024
Fernada Riffo	COO	12/04/2024

Roles y Responsabilidades

Responsabilidades respecto de la gestión de la seguridad:

Rol	Responsabilidad
Comité Directivo	Revisar y aprobar las actualizaciones de la presente política al menos una vez al año.
Comité Operativo	Realizar actividades y supervisar a colaboradores y proveedores a su cargo, para garantizar el cumplimiento de la presente política.

Head of Security	Revisar el cumplimiento, revisar la eficiencia y actualizar la presente política al menos una vez al año.
Colaboradores y Proveedores	Cumplir la presente política.

RACI

Roles	Responsable	Aprobador	Consultado	Informado
Comité Directivo		■		
Comité Operativo	■			
Head of Security	■			
Colaboradores				■
Proveedores				■
Consultores SGSI			■	
Autoridades				■
Clientes				■
Público en general				■

Contactos

Lista de roles notables:

Sujetos	Contactos	Teléfono	Email
Head of Security	Diego González	+593998981436	diego.gonzalez@rankmi.com

Términos y Definiciones

Términos	Definiciones
Dispositivo de usuario final	Dispositivo de hardware de Tecnología de información y comunicaciones (TIC) conectado a la red.