

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

Esta Política de Seguridad de la información define los lineamientos y medidas a tener en cuenta para gestionar los riesgos de seguridad de la información sobre los activos de información, los procesos y actividades del negocio.

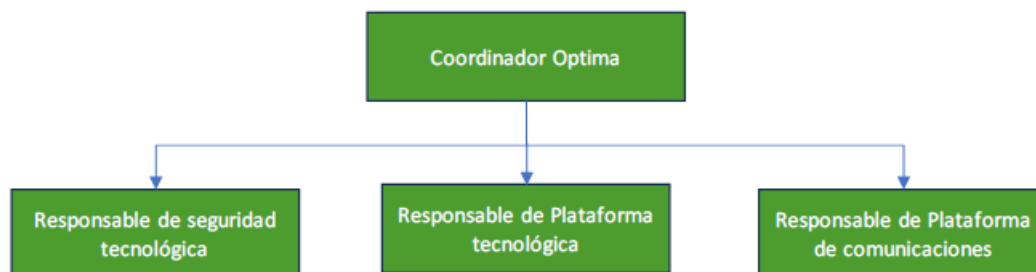
1.1. Objetivo

Establecer las políticas, prácticas y lineamientos que permitan a la organización garantizar la adecuada protección de todos sus activos de información y prevenir la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.

1.2 Alcance

Esta Política de Seguridad de la Información es aplicable a todos los activos de información de la compañía, así como a todos los procesos, actividades de negocio y a todas las personas que directa o indirectamente prestan algún servicio para la organización.

1.3 Roles



Coordinador

Es la persona responsable de la correcta ejecución del plan de continuidad de TI formado debe confirmar la orden de inicio en la ejecución del plan de continuidad, coordinar las actividades de contingencia con los diferentes integrantes del equipo responsable del plan de continuidad de TI, seguir el estado de las estrategias aplicadas, y confirmar el cierre del plan y retorno a la normalidad.

Entre sus responsabilidades se encuentran:

- Ejecutar el plan de continuidad, previa confirmación de activación.
- Reunir al equipo responsable del plan en el punto de encuentro, en caso de ser necesario.
- Realizar un análisis conjunto de la situación.
- Coordinar los lugares y personas donde se ejecutará el plan.
- Mantener contacto con todas las personas responsables internas y externas involucradas.
- Supervisar la correcta implementación de las actividades requeridas del plan de continuidad de TI.

Política de seguridad de la información

- *Supervisar con el personal de seguridad que las personas acaten las indicaciones de emergencia que se les indique y atender a los usuarios internos y externos afectados.*
- *Hacer seguimiento del estado de la operación de los servicios y actividades en contingencia.*
- *Supervisar el retorno a la normalidad de la operación de las áreas afectadas, documentar acciones y lecciones aprendidas, y confirmar el cierre del plan.*

Responsable de seguridad tecnológica

Es la persona responsable del cumplimiento normativo y operativo de los procesos, sistemas y activos tecnológicos relacionados con la seguridad de la información.

Entre sus responsabilidades está:

- *Realizar una inspección conjunta de los activos de tecnología que soportan la seguridad de la información.*
- *Coordinar el uso y restauración de respaldos de información.*
- *Hacer seguimiento del uso y control de acceso de la plataforma tecnológica.*
- *Coordinar la restauración de perfiles de usuario, permisos de uso y gestión de información.*
- *Hacer seguimiento de la configuración de activos que se requiera instalar.*
- *Sí aplica preparar perfiles temporales para el personal que requiera trabajar.*
- *Supervisar el traslado de activos tecnológicos, físicos y de información a sitios alternos, y certificar el retorno de dichos activos.*
- *Certificar las condiciones de seguridad, disponibilidad, confidencialidad e integridad de la información.*

Responsable de la plataforma tecnológica

Es la persona responsable de validar la integridad y disponibilidad de los activos que componen la plataforma tecnológica, estos son: servidores físicos y virtuales, unidades de almacenamiento, repositorios, servicios de tecnología e información digital y unidades de creación de respaldo.

Entre sus responsabilidades está:

- *Inspeccionar los activos que componen la plataforma tecnológica, principalmente centro de datos y sitios alternos de procesamiento de información.*
- *Evaluar la integridad de los activos de tecnología.*
- *Coordinar las actividades relacionadas con la recuperación de servidores físicos, virtuales y repositorios.*
- *Coordinar las actividades relacionadas con la recuperación funcional de los servicios de tecnología de la institución.*
- *Coordinar la configuración de activos de procesamiento de información que se requieran como activos para contingencias.*
- *Certificar el funcionamiento correcto de los activos de tecnología previo al cierre del plan de continuidad.*

Responsable de la plataforma de comunicaciones

Es la persona responsable de validar la integridad y disponibilidad de los activos que componen la plataforma de comunicaciones, estos son: switches, routers, central y unidades de telefonía, enlaces de comunicación, cableado de datos y voz, VPN.

Entre sus responsabilidades está:

- *Inspeccionar los activos que componen la plataforma de comunicaciones, principalmente centro de datos y sitios alternos de procesamiento de información.*
- *Evaluar la integridad de los activos de comunicación.*

2. Privacidad de los datos

Datos personales que recopilamos

Podemos recopilar datos personales directamente de usted, de terceros o de datos disponibles públicamente, o automáticamente cuando usted utiliza los Sitios mediante el uso de tecnologías como protocolos de comunicación electrónica, cookies, botones de widgets o herramientas.

Recogemos estos datos personales para los fines que se describen a continuación.

Cómo utilizamos los datos personales

Sólo utilizaremos sus datos personales si tenemos una base legal para hacerlo. En concreto, utilizamos sus datos personales siguiendo sus instrucciones o de la siguiente manera: Proporcionar y personalizar nuestros Sitios. Para operar y administrar los Sitios y proporcionarle el contenido al que decide acceder o solicitar; para adaptar el contenido de la web que le mostramos con el fin de ofrecer la personalización de la ubicación (por ejemplo, establecer un idioma por defecto) y para personalizar de otro modo su experiencia al utilizar los Sitios. Podemos utilizar cookies y tecnologías de seguimiento similares para recopilar automáticamente sus datos personales con este fin.

3. Acceso remoto / inalámbrico. Conectividad de terceros

Es responsabilidad de los empleados, contratistas, proveedores y agentes de OPTIMA con privilegios de acceso remoto a la red corporativa de OPTIMA garantizar que su conexión de acceso remoto tenga la misma consideración que la conexión in situ del usuario a OPTIMA.

El acceso general a Internet para uso recreativo por parte de los miembros inmediatos de la familia a través de la red de OPTIMA en ordenadores personales está permitido para los empleados que tienen servicios de tarifa plana. El empleado de OPTIMA es responsable de garantizar que el miembro de la familia no infrinja ninguna política de OPTIMA, no realice actividades ilegales y no utilice el acceso para intereses comerciales externos.

El empleado de OPTIMA es responsable de las consecuencias en caso de que el acceso se utilice de forma indebida.

4. Estándares de encriptación, seguridad perimetral/red, seguridad personal, control de accesos

Mediante la codificación de documentos y comunicaciones, un concepto sofisticado de derechos, restricciones de acceso y auditorías de seguridad, DocuWare Cloud garantiza la seguridad de sus datos.

En un centro de datos utilizado por DocuWare, todos los datos del cliente están protegidos mediante una VPN (Virtual Private Network). La infraestructura de red también está virtualizada y la red virtual está protegida desde el exterior.

Para la codificación del tráfico de datos entre los usuarios y el centro de datos, se utiliza el protocolo TLS actual (protocolo sucesor de SSL), siempre y cuando resulte compatible con el navegador correspondiente. TLS se utiliza para todo el tráfico basado en HTTP (HTTPS) y TCP. Los usuarios consultan inmediatamente en el navegador si su conexión está asegurada y válida: En una conexión segura, la barra de URL se vuelve verde (a excepción de Google Chrome).

Encriptación de Datos:

COMUNICACIONES: Cortar comunicaciones Externas e internas buscar la vulnerabilidad o intrusión y realizar correcciones.

Política de seguridad de la información

SERVIDORES: Realizar inventario de los servidores infectados he aislarlos de la red para que no se extienda el software malicioso.

Restaurar copias de seguridad en servidor replicas si fuera necesario.

5. Antivirus

Actualmente los servidores de la compañía se encuentran protegidos por un antimalware con tecnología EDR SOPHOS, además de estar protegidos mediante el Firewall.

A nivel de endpoint también utilizamos tecnología EDR de Sophos.

6. Correo electrónico/mensajería instantánea

Todo uso del correo electrónico debe cumplir con las políticas de la empresa sobre conducta ética y seguridad de los datos empresariales.

Todo uso del correo electrónico debe estar en consonancia con las prácticas empresariales adecuadas y ser relevante para las funciones del trabajo.

Las direcciones de correo electrónico o los sistemas de la empresa no se utilizarán para crear, distribuir o acceder a ningún material ofensivo o ilegal, incluido, entre otros, el material con comentarios ofensivos sobre el género, la raza, la edad, la orientación sexual o las creencias religiosas.

Cualquier material ofensivo que se reciba por correo electrónico deberá ser comunicado al Departamento de TI y a Recursos Humanos sin demora.

El uso de las direcciones y sistemas de correo electrónico propiedad de la empresa para uso personal debe limitarse a un uso mínimo e incidental.

Se prohíbe el uso de direcciones de correo electrónico o sistemas propiedad de la empresa para usos comerciales o relacionados con el negocio que no formen parte de la actividad de la empresa.

El correo electrónico recibido en las direcciones de correo electrónico de la empresa no puede reenviarse automáticamente a direcciones de correo electrónico que no sean propiedad de la empresa o que no estén operadas por ella.

Las direcciones de correo electrónico individuales reenviadas a direcciones de correo electrónico que no sean propiedad o estén operadas por la empresa no deben contener ninguna información sensible o confidencial.

Se prohíbe la creación o el reenvío de cadenas o cartas de broma desde direcciones de correo electrónico o sistemas de la empresa.

La empresa puede supervisar y registrar todos los mensajes de correo electrónico recibidos o enviados por las direcciones de correo electrónico o los sistemas propiedad de la empresa o gestionados por ella.

La empresa no supervisa necesariamente toda la actividad del correo electrónico, pero se reserva el derecho a hacerlo.

Con fines de análisis y mejora de la atención al cliente, la compañía podrá utilizar sistemas de inteligencia artificial propios y/o de terceros autorizados. Cualquier tratamiento de información realizado mediante dichos sistemas deberá incorporar, desde su inicio o en las primeras fases del proceso, medidas de minimización de datos, seudonimización y, cuando resulte posible, anonimización, con el fin de reducir la exposición de datos personales.

Política de seguridad de la información

7. Seguridad física

Los puestos de trabajo, tanto fijos como móviles, estarán bajo la responsabilidad del usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

Contamos con una empresa externa para el custodio de las copias de seguridad.

Estas están ubicadas en un bunker protegido con autenticación biométrica y personal muy específico.

8. Gestión de Dispositivos Móviles (MDM) con Samsung Knox

IMPLEMENTACIÓN DE SAMSUNG KNOX: Todos los dispositivos móviles Samsung deben estar registrados en la plataforma Samsung Knox para su gestión. La configuración y el despliegue de políticas de seguridad serán administrados centralizadamente por el departamento de TI.

CONTROL DE ACCESO: Se utilizarán las funcionalidades de bloqueo de Knox, como el bloqueo de pantalla, autenticación biométrica y contraseñas robustas, para asegurar un acceso seguro al dispositivo.

PROTECCIÓN DE DATOS: Activar el cifrado proporcionado por Knox en todos los dispositivos para proteger los datos almacenados y en tránsito. Esto incluye el uso de VPNs seguras para el acceso remoto a la red corporativa.

GESTIÓN DE APLICACIONES: Solo se permitirá la instalación de aplicaciones aprobadas y verificadas por el departamento de TI. Las aplicaciones deberán ser gestionadas a través de la tienda de aplicaciones de Knox para asegurar su integridad y seguridad.

ACTUALIZACIONES Y PARCHES DE SEGURIDAD: Los dispositivos deben configurarse para recibir y aplicar automáticamente las actualizaciones de software y parches de seguridad proporcionados por Samsung Knox, para proteger contra vulnerabilidades conocidas.

RESPUESTA A INCIDENTES: En caso de pérdida o robo de un dispositivo, se deben seguir los procedimientos de respuesta a incidentes establecidos, incluyendo la capacidad de borrado remoto y bloqueo del dispositivo a través de Samsung Knox.

FORMACIÓN Y CONCIENCIACIÓN: Proporcionar formación regular a todos los usuarios de dispositivos móviles Samsung sobre las políticas de seguridad, mejores prácticas y cómo utilizar de manera segura las funcionalidades de Knox.

OPTIMA FACILITY SL
OPTIMA FACILITY SERVICES SLU
OPTIMA TECHNICAL SERVICES SAU
OPTIMA INCLUSION Y DIVERSIDAD SL
PEOPLE PLUS INNOVATION SL
SERVICIOS OPERATIVOS INTERNOS SAU
ELECTRICA INSTALADORA SLU
L'HEURA, CENTRE ESPECIAL DE TREBALL SL
HEURA INCLUSION Y DIVERSIDAD SL
VENTURE TECH INNOVATIONS SL

Enero 2026

Ignasi Casamada Bragulat
CEO & Co-Founder

