heura

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Uso aceptable

La Política de Uso Aceptable de **HEURA**, especifica las acciones prohibidas a los usuarios de la red, reservándose el derecho de modificar dicha Política en cualquier momento, siendo de obligado cumplimiento dichas modificaciones a partir de la publicación.

HEURA, pondrá todos sus esfuerzos para que la Política de Uso Aceptable se respete y cumpla por los usuarios y/o clientes que tengan acceso a la misma como normas básicas, con la finalidad de preservar los bienes, servicios y funcionamiento de la Red y abstenerse de forma expresa del uso de los servicios con fines ilícitos y/o poco éticos.

Privacidad de los datos

HEURA, puede recopilar datos personales de sus trabajadores, de terceros o de datos disponibles públicamente.

El tratamiento de datos se realiza para el cumplimiento de obligaciones legales por parte de **HEURA**, para el cumplimiento de misiones realizada en interés público o en el ejercicio de poderes públicos conferidos a la **HEURA** así como cuando la finalidad del tratamiento requiera su consentimiento, que habrá de ser prestado mediante una clara acción afirmativa

Acceso remoto / inalámbrico, conectividad de terceros

Es responsabilidad de los trabajadores, proveedores y subcontratas de **HEURA** con privilegios de acceso remoto a la red corporativa de **HEURA**, garantizar que su conexión de acceso remoto tenga la misma consideración que la conexión in situ del usuario a **HEURA**.

El acceso general a Internet para uso recreativo por parte de los miembros inmediatos de la familia a través de la red de **V** en los ordenadores personales está permitido.

El empleado de **HEURA** es responsable de garantizar que el miembro de la familia no infrinja ninguna política de **HEURA**, no realice actividades ilegales y no utilice el acceso para intereses comerciales externos.

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

Respuesta a incidentes de seguridad

HEURA en referencia a este punto dispone de un plan de contingencia IT con un enfoque explícito en incidentes de ciberseguridad.

Contamos con un equipo el cuál dispone de certificación de *Secure Deveolpment Awarness*.

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

HEURA 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 validada: 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.

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.

Antivirus

Actualmente los servidores de la compañía se encuentran protegidos por el Antivirus Eset y Sophos, además de estar protegidos mediante el Firewall.

Al igual que los usuarios cuentan con protección a través de Sophos y ESET.

Correo electrónico/mensajería instantánea

Todo uso del correo electrónico debe cumplir con las políticas de **HEURA** 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 **HEURA** 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 IT y de Personas y Valores sin demora.

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

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

El correo electrónico recibido en las direcciones de correo electrónico 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 **HEURA**.

HEURA puede supervisar y registrar todos los mensajes de correo electrónico recibidos o enviados por las direcciones de correo electrónico o los sistemas propiedad gestionados por ella; no supervisa necesariamente toda la actividad del correo electrónico, pero se reserva el derecho a hacerlo.

heura

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

Abril 2023
DIRECCION GENERAL