Política de Seguridad del sitio Cuprum

2023

Cuprum afp

Una compañía Principal®

Índice de contenidos

1. Introducción.

Por intermedio de la presente declaración, CUPRUM AFP informa a los usuarios del sitio web que la información que conserva con nosotros se mantiene segura y confidencial mediante varias características y procedimientos de seguridad. Así mismo informa a los usuarios del sitio sobre la importación de tomar medidas personales para proteger tu información y así reducir riesgos a la seguridad de la información.

2. Características de seguridad online que ayudan a proteger tus datos.

La información que solicitas mediante nuestro sitio web sobre tus cuentas sólo se puede acceder con tus credenciales de accesos (usuario y contraseña). Es tu responsabilidad y la de esta administradora mantener esta información confidencial.

- No compartas tu información de ingreso con nadie. Nuestros empleados nunca te pedirán tu contraseña completa.
- Si escribes tu información de ingreso, mantenla guardada en un sitio seguro donde nadie la pueda obtenerla.
- Comunícate con nosotros inmediatamente para cambiar tus claves de accesos si sospechas que alguien la ha descubierto.
- Recuerda proteger tu información de contacto (accesos a tu cuenta de correo, número telefónico, entre otros), para evitar fraude a través de esos canales que puedan afectar tus cuentas con nosotros.

La información que brindas a través de nuestro sitio web, así como la información que te mostramos en él mientras lo visitas, está protegida en su recorrido por Internet mediante un fuerte encriptado (para que sea incomprensible) cuando es necesario. Nuestro software de servidor seguro encripta la información para asegurarse que las comunicaciones por Internet a través de nuestro sitio web se mantengan privadas y protegidas.

Para que nuestros clientes puedan procesar transacciones en nuestro sitio web, utilizamos cookies. La información de tu cuenta no queda almacenada permanentemente en nuestro servidor web, sino que reside en él solamente mientras estés viendo dicha información. Esta información queda permanentemente almacenada en nuestros sistemas informáticos seguros internos.

3. Softwares de seguridad que ayudan a proteger tu información.

Para garantizar la transmisión segura de la información confidencial de tu cuenta a través de Internet, utilizamos una solución de comunicaciones segura llamada Seguridad de la Capa de Transporte (Transport Layer Security – TLS por sus siglas en ingles). Todos los navegadores modernos admiten TLS, pero si tu navegador no lo hace, recibirás un mensaje que indica que tu inicio de sesión no se puede completar debido al riesgo de seguridad.

El protocolo TLS establece una conexión segura entre dos partes (por ejemplo, tu navegador y nuestro servidor web). Se utiliza para implementar el protocolo seguro de transferencia de hipertexto HTTPS (en inglés: Hypertext Transfer Protocol Secure), la versión segura de HTTP, y es una tecnología abierta compatible con diversos navegadores (por ejemplo, Microsoft Edge o Google Chrome).

CUPRUM AFP requiere que utilices un navegador habilitado con TLS para que te comuniques con el área segura de nuestro sitio. Sabrás que estás visitando el área segura de nuestro sitio si la dirección Web (URL) comienza con "https://...".

Para brindarte un alto nivel de seguridad, te recomendamos el uso de los navegadores más actuales que sean compatibles con la más reciente tecnología de encriptado.

Además de proteger las comunicaciones entre tu navegador y nuestro servidor, el protocolo TLS también se utiliza para proteger las comunicaciones entre nuestro servidor web y nuestro sistema central. De igual forma, hemos implementado un cortafuegos (o “firewall”) para proteger todos nuestros sistemas que no sean parte de Internet contra cualquier intrusión.

4. Limitamos el acceso a los datos

CUPRUM AFP tiene políticas y procedimientos establecidos para limitar el acceso a tu información a solo aquellas personas que tengan una necesidad de negocio. Tenemos proceso formal y documentado para otorgar y revocar el acceso a los recursos de la empresa (sistemas, datos, dispositivos, etc.) que están respaldados por controles administrativos, técnicos y físicos.

Nuestros sistemas de red, que almacenan tu información utilizan probados controles de seguridad. Tenemos personal para la seguridad de los datos cuya responsabilidad es garantizar la seguridad de la información que procesamos y almacenamos.

5. Otras formas como protegemos tu información.

A continuación, te presentamos otros elementos con los que cuenta CUPRUM AFP para proteger tu información.

5.1. Encriptado.

Las computadoras portátiles de CUPRUM AFP están encriptadas, al igual que la transmisión de toda la información confidencial. Dicha transmisión se realiza a través de conexiones seguras, como:

- Protocolo seguro de transferencia de hipertexto o HTTPS a través del TLS (en inglés: Hypertext Transfer Protocol Secure).
- Protocolo de transferencia segura de archivos o SFTP (En inglés, Secure File Transfer Protocol) a través de Internet.
- Encriptado PGP (Pretty Good Privacy) a través del SFTP.

5.2. Programa de seguridad.

CUPRUM AFP tiene un programa de seguridad de la información que protege la información contra modificaciones, revelaciones, fraudes y destrucción no autorizados o accidentales.

- Las políticas de seguridad, las normas y los procedimientos están documentados y disponibles para nuestros empleados.
- La recopilación de información personal se limita a las necesidades comerciales y se protege en función de su sensibilidad.
- Los empleados deben completar la capacitación sobre privacidad, seguridad, ética y cumplimiento.
- Las evaluaciones del área de trabajo se completan para garantizar la protección de la información y los sistemas de información.
- Los procesos y procedimientos de gestión de riesgos están documentados y comunicados. Los riesgos emergentes a la seguridad de la información, incluyendo los de ciberseguridad, son revisados a fin de evaluar la necesidad de realizar cambios a nuestras prácticas de seguridad.

5.3. Protección antivirus

Todos los servidores y estaciones de trabajo Windows tienen instalado un software antivirus y las actualizaciones de las definiciones de virus se aplican con frecuencia. Nuestros gerentes de tecnología de la información revisan los informes regularmente para garantizar que se cumplan los niveles de cumplimiento. Todas las alertas son revisadas por el personal en el centro de operaciones de ciberdefensa.

5.4. Gestión de parches

Supervisamos las nuevas vulnerabilidades y ataques significativos que pueden afectar a nuestros sistemas y aplicamos parches según corresponda. Tenemos una práctica de administración de vulnerabilidades que prueba nuestros sistemas con regularidad para garantizar que no estén abiertos a ataques.

5.5. Administración de incidentes

Tenemos procesos para rastrear, administrar y resolver todos los incidentes. Todos los incidentes son investigados. Si se descubre un incidente de seguridad de datos, un plan de respuesta se inicia rápidamente y se ejecuta a fondo. Se consideran especialmente relevantes los incidentes de Ciberseguridad, pues pueden estar asociados a riesgos emergentes que pueden dar origen a una revisión de nuestras prácticas de seguridad.

5.6. Colaboración de la industria

Principal es miembro del Centro de Servicios y Análisis de Información Financiera (FS-ISAC). FS-ISAC es un foro de la industria para la colaboración en amenazas de seguridad críticas que enfrenta la industria global de servicios financieros. CUPRUM AFP es miembro de Principal y por lo tanto goza de los beneficios de dicha membresía.

5.7. Prácticas de seguridad adicionales

- Los centros de llamada tienen procedimientos establecidos para ayudar a validar la identidad de las personas que nos llaman.
- Capacitamos periódicamente a nuestros empleados sobre cómo detectar actividades fraudulentas.
- Seguimos estándares para limitar el acceso a los datos.
- Probamos nuestra tecnología de seguridad periódicamente

Si tienes más preguntas o comentarios sobre seguridad, por favor comunícate con nosotros.

6. Tú también puedes ayudar a proteger tu información

Además de los pasos que implementamos en CUPRUM AFP para que la información de tu cuenta esté segura, las medidas que tú tomas son cruciales para protegerte.

La protección de tu información personal puede ayudar a reducir el riesgo de robo de identidad. Hay cuatro formas principales de hacerlo:

1. Sepa con quién comparte información.
2. Almacene y elimine tu información personal de forma segura.
3. Haga preguntas antes de decidir compartir tu información personal.
4. Mantenga la seguridad adecuada en tus computadoras y otros dispositivos electrónicos como celulares y tablets.
5. Privilegia el uso de doble factor de autenticación para el ingreso a los sistemas y dispositivos. Generalmente el primer factor de autenticación son tus credenciales de accesos (Usuario y contraseña) y el segundo factor suele ser una clave dinámica que te puede llegar al celular o al correo electrónico.

6.1. Protege tus credenciales de acceso

- Nunca compartas tu clave de acceso o clave de seguridad. Sé cauteloso con los emails y las personas que piden esta información. CUPRUM AFP nunca te pedirá tu contraseña personal enviándote un email ni llamándote por teléfono o a través de SMS.
- Oculta el teclado con tu mano o cuerpo al momento de ingresar tus claves de accesos.
- Cambia las contraseñas regularmente utilizando una combinación de números y caracteres. Tu contraseña es más segura y difícil de adivinar para un delincuente si le incluyes caracteres especiales, como un asterisco o un signo de exclamación.
- Revisa y verifica tus estados de cuenta con frecuencia. Pon atención a cualquier transacción o comunicación que recibas de CUPRUM AFP. Revisa la actividad de tus cuentas a menudo.

6.2. Protege tu información personal contra virus

Tu computadora personal:

Es probable que uses el computador de tu hogar para conectarte en línea a internet para verificar tus cuentas con nosotros y hacer negocios con otras compañías. Por eso es

importante protegerlo de virus y spyware. La mayoría de las compañías de software lanzan regularmente actualizaciones o parches a sus sistemas operativos para reparar problemas de seguridad. Es una buena idea mantener tu sistema y tus aplicaciones actualizadas con los últimos parches y versiones.

Tus dispositivos móviles:

Que no se te olvide la seguridad de tu teléfono inteligente y tableta, es tan importante como una computadora personal.

Siempre active un PIN o función de bloqueo para tu dispositivo. Esta es la cosa más simple e importante que puedes hacer para garantizar la seguridad en tu dispositivo móvil, especialmente si se pierde o es robado.

Tenga cuidado al descargar aplicaciones. Evite instalar aplicaciones fuera de las tiendas de aplicaciones de Apple o Google. Algunas aplicaciones pueden contener malware (Software malintencionado) diseñado para robar tu información personal y financiera. Antes de instalar la aplicación, revise los permisos para decidir si está cómodo otorgando el nivel de acceso solicitado por esa aplicación. También es una buena idea ver la calificación de la aplicación, leer las opiniones de otros usuarios y los comentarios para ver si se ha informado algo sospechoso sobre la aplicación.

6.3. Seguridad en línea

El uso de una red inalámbrica en el hogar es conveniente, pero dejarlo sin seguridad es una oportunidad para que los ciberdelincuentes accedan y descubran tu información confidencial. Asegúrate de usar un código de acceso único para que tu familia sea la única que use la red. También puede comunicarse con tu proveedor de servicio inalámbrico para obtener un cifrado más robusto.

6.4. Salir de un sitio web

Después de ingresar a una página web con tus credenciales de accesos, recuerda cerrar sesión. Es un paso fácil que puede tomar para asegurarse de que tu información no termine en las manos equivocadas.

6.5. Elige una contraseña segura

- No utilices la misma contraseña en otros sitios web de información más sensible, como la banca online. Si otros sitios no son seguros, tu contraseña podría verse comprometida.
- Elige contraseñas que no sean iguales a otra información personal, por ejemplo, números de identidad (RUT), fecha de nacimiento, etc.

- Elige contraseñas que sean fáciles de recordar para ti, pero difíciles de adivinar para otros. No utilices información sobre ti que otros puedan descubrir fácilmente.
- Utiliza al menos 8 caracteres. En la medida de lo posible, es buena idea variar los tipos de caracteres de tus contraseñas. Las combinaciones de mayúsculas, números y símbolos hacen que las contraseñas sean mucho más difíciles de adivinar.
- Utiliza segundo factor de autenticación como claves dinámicas en caso de que el servicio lo soporte.

¿Has sido víctima de un fraude o sospechas de la vulneración de tus credenciales de accesos?

Haz tu reporte a través de nuestras canales oficiales de comunicación, como lo son el centro de atención telefónica, página web u oficina.

7. Manejo de versiones.

Versión	Fecha Vigencia	Fecha última Actualización	Modificaciones
1	Junio 2019	03-06-2019	Creación de la política
2	Septiembre 2021	08-09-2021	Se actualizan navegadores seguros con compatibilidad https.
3	Octubre 2023	11/10/2023	Sin cambios en el documento, se ratifica versión actual.

8. Control del documento.

Elaborado por	Gerente de Tecnología
Revisado por	Comité de Riesgo y Auditoria (CRA)
Aprobado por	Directorio