20 AÑOS CONEXA
FINANCIAL GROUP

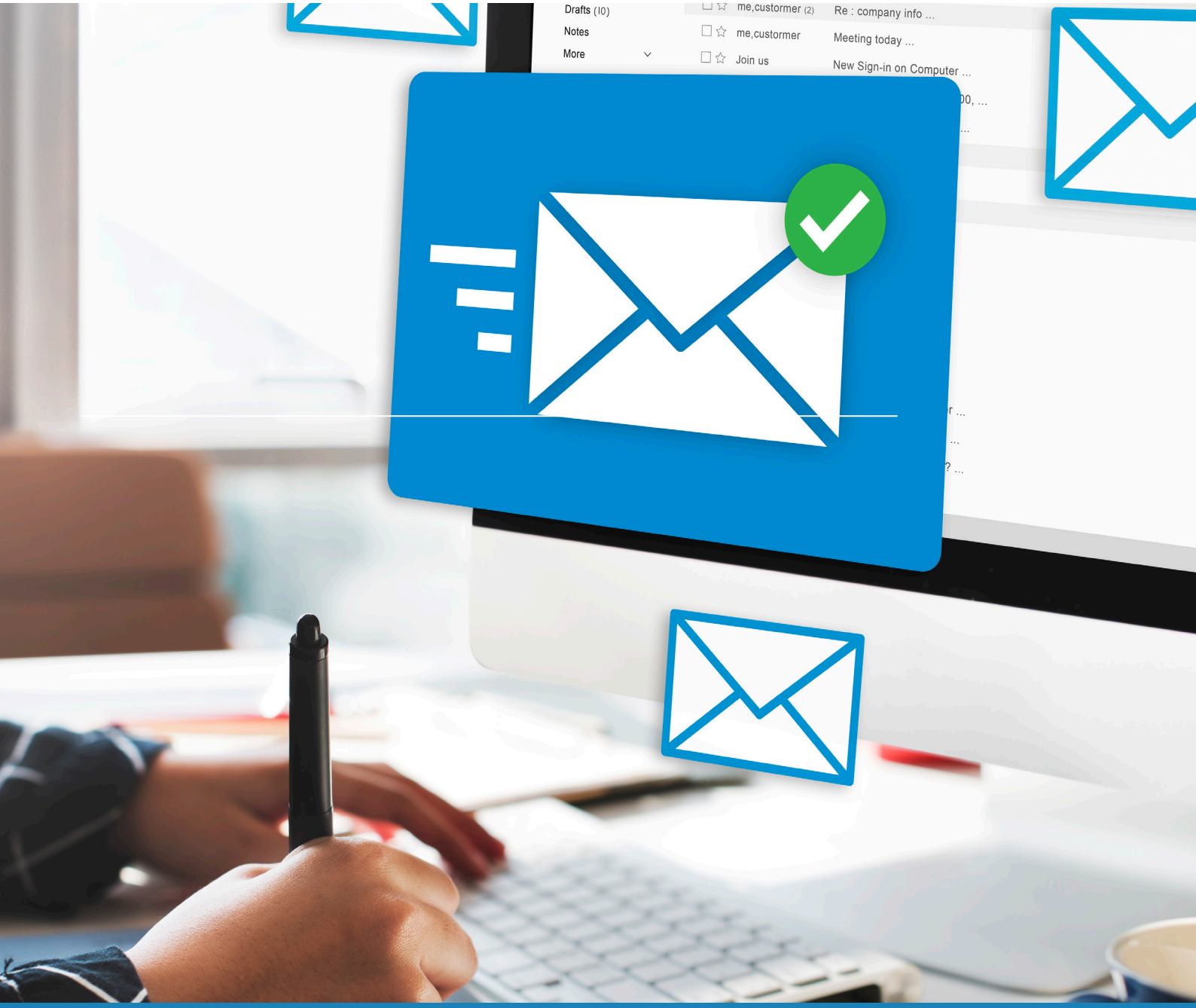
SISTEMA DE SEGURIDAD DE INFORMACIÓN

Guía de Seguridad de la Información Conexa 2024

Área de Seguridad de la Información

Gerencia de Finanzas, Fondos, Operaciones y TI

20 AÑOS CONEXA FINANCIAL GROUP



Objetivo

Proteger la información de la empresa, es responsabilidad de todos nosotros.

Desde el correo electrónico que recibimos a diario hasta los documentos que manejamos, cada uno tiene un papel crucial en **mantener la seguridad de la empresa.**

1

¿Qué es la Seguridad de la Información?

Es un conjunto de medidas preventivas que permiten proteger la información con el fin de mantener la confidencialidad, integridad y disponibilidad de la información.

¿Cuáles son los pilares de la Seguridad de la Información?

Existen tres pilares de la Seguridad de la Información:

Confidencialidad: garantizar que la información sea accesible sólo por aquellas personas autorizadas.

Integridad: salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento y transmisión.

Disponibilidad: garantizar que la información se encuentre a disposición de quienes deben acceder a ella.

Recuerda que la confidencialidad, integridad y disponibilidad están en nuestras manos.

¡Con pequeños hábitos podemos proteger la seguridad de la empresa!

¿Qué es un Sistema de Gestión de la Información (SGSI)?

Es un conjunto de políticas, procedimientos y controles que una empresa implementa para gestionar y proteger su información de manera sistemática. Este sistema ayuda a identificar, gestionar y minimizar los riesgos relacionados con la seguridad de la información.

Esta se encuentra en la norma ISO/IEC 27001 – Seguridad de la Información.

¿Quiénes forman parte del Sistema de Gestión de Seguridad de la Información?

En el Sistema de Gestión de Seguridad de la Información lo conforman todos los empleados de Conexa.

Guía de Seguridad de la Información Conexa 2024

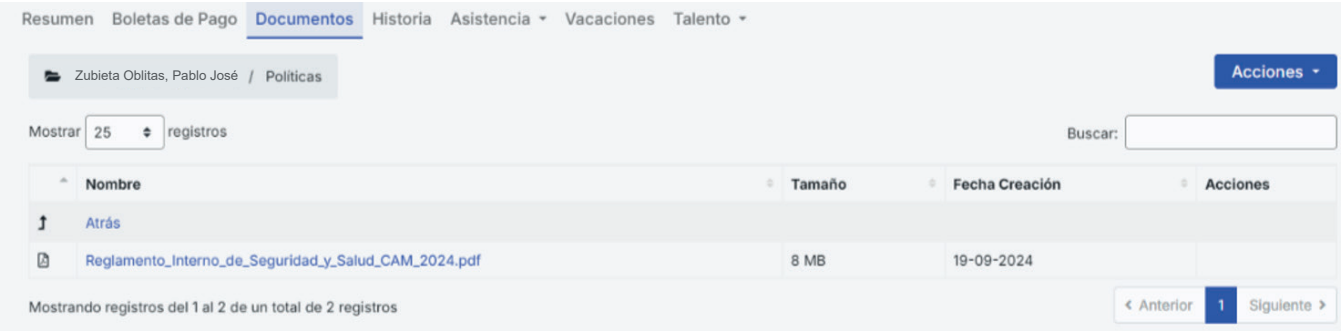
¿Qué es la política de Seguridad y Confidencialidad de la Información?

Es un conjunto de reglas y directrices que la empresa establece para proteger sus activos de información y garantizar que solo las personas autorizadas accedan a los datos sensibles.

¿Dónde puedo encontrar los documentos relacionados a la Gestión de Seguridad de la información?

Toda la documentación relacionada la podemos encontrar en la plataforma BUK, en la sección de documentos.

Dentro de la sección podrás encontrar nuestras **Políticas, Manuales, Reglamentos, Normas, Procedimientos** relacionados a la **Gestión de la Información.**



¡ES IMPORTANTE! Conocer y cumplir con las normativas de Seguridad de la Información.

2

Activos de Información

Guía de Seguridad de la Información Conexa 2024

¿Qué son los activos de información?

Cualquier recurso o activo que se utiliza para la operación y cumplimiento de los objetivos propuestos por la empresa.

Todo activo de información debe ser identificado y clasificado en función a los niveles requeridos de confidencialidad, integridad y disponibilidad, requerimientos legales, normativos y de negocio.

¿Cuáles son los recursos de información?

Pueden ser físicos o digitales, software, hardware, proveedores y personas.

¿Cómo se encuentra clasificada la información?

Pueden ser físicos o digitales, software, hardware, proveedores y personas.

Pública

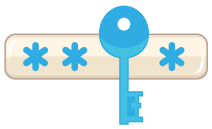
Información considerada de valor, pero no existe riesgo de acceso no autorizado.

Interna

Información que son solo para uso interno de la empresa, pero que no requieren un alto nivel de protección.

Confidencialidad

Información que solo pueden ser compartidos con personas autorizadas dentro de la empresa.



Restringida

Información con el más alto nivel de sensibilidad dentro de Conexa. El acceso a esta información debe ser debidamente autorizada y justificada.

Tratamiento de la información

Antes de compartir información confidencial y restringida deben asegurarse de que el destinatario se encuentre autorizado. La información confidencial y restringida siempre debe compartirse de manera segura.

3

Normas de Control de Accesos

Guía de Seguridad de la Información Conexa 2024

¿Qué requisitos debo cumplir para tener mayor seguridad en las contraseñas de mis cuentas?

- Lo recomendable es tener contraseñas de al menos 8 caracteres o dígitos, pero cuanto más largas mejor.
- Asegúrate de que tus contraseñas incluyan una mezcla de letras mayúsculas, minúsculas, números y símbolos.
- Evita la reutilización de contraseñas antiguas.
- No compartas tu contraseña con ningún otro colaborador.
- Activa la autenticación de dos factores (2FA).

De acuerdo con la Norma de Control de Accesos. ¿Qué debo hacer antes de alejarme de mi computadora?

- Deberás bloquear tu pantalla antes de alejarte.
- Terminar todas las sesiones de las aplicaciones y programas de información que están activas.
- Cierra documentos confidenciales y no compartas contraseñas.

Si tengo acceso al correo electrónico corporativo. ¿Cuál es el manejo correcto del mismo?

El uso del correo corporativo debe ser exclusivamente para fines laborales, manejando la información confidencial con cuidado y evitando abrir correos sospechosos o spam.

En caso de adjuntar información confidencial y/o restringida deben estar autorizado por el jefe inmediato, y siempre debe compartirse de manera segura.

¿Estoy cometiendo alguna falta si intento ingresar al sistema probando posibles contraseñas de otras cuentas?

¡Sí, estás cometiendo una falta grave! Intentar ingresar a cuentas ajenas probando diferentes contraseñas, incluso si lo haces por curiosidad o con buenas intenciones, es considerado un acceso no autorizado. Esto puede tener consecuencias tanto para ti como para la empresa.

¿Por qué es tan grave?

Viola las políticas de seguridad: Toda empresa tiene reglas claras sobre el acceso a la información y los sistemas. Intentar acceder a cuentas sin permiso infringe esas reglas y puede resultar en medidas disciplinarias serias.

Es ilegal: Dependiendo del país, intentar acceder a una cuenta ajena sin autorización es un delito, incluso si no logras entrar. Podrías enfrentarte a consecuencias legales como multas o cargos criminales, lo que impactaría seriamente tu historial personal y profesional.

Atenta contra la privacidad: Cada empleado tiene derecho a la privacidad de su información. Tratar de acceder a la cuenta o la computadora de otra persona puede considerarse una violación de su confidencialidad y puede crear problemas de confianza entre colegas.

Poner en riesgo la seguridad de la empresa: Al probar diferentes contraseñas, puedes activar alertas de seguridad, bloquear cuentas de manera involuntaria o incluso debilitar la protección del sistema, lo que afecta a toda la organización.

¿Qué deberías hacer en lugar de esto?

Si tienes problemas para acceder a tu cuenta, utiliza los métodos de recuperación de contraseña de manera segura o pide ayuda al departamento de TI.

4

Incidencias de información comprometida

La información comprometida es uno de los mayores riesgos a los que cualquier empresa puede enfrentarse. Esto ocurre cuando datos sensibles o confidenciales se ven expuestos, robados o manipulados por personas no autorizadas, lo que puede tener graves consecuencias tanto a nivel interno como externo.

¿Qué significa que la información esté comprometida?

Cuando decimos que la información está "**comprometida**", hablamos de cualquier situación en la que:

- ⚠ Datos confidenciales (como información de clientes, empleados o proyectos) son accedidos sin autorización.
- ⚠ Se produce una filtración de información, ya sea por descuido, un ataque externo o por acciones malintencionadas.
- ⚠ Los archivos o sistemas de la empresa han sido alterados o manipulados sin consentimiento.

¿Existen sanciones cuando se cometen acciones que provoquen incidentes de seguridad de información?

Sí, las acciones que provoquen un incidente de seguridad de información y son considerados como fraude, pueden ser causal de amonestaciones.

Tengo sospechas sobre una violación a los lineamientos de seguridad de la Información. ¿Qué debo hacer?

Deberás informar inmediatamente a tu jefe inmediato.

El sistema me permite hacer actividades que a mi compañero de mí mismo cargo no. ¿Puedo hacer uso de estos permisos?

No, los accesos que no corresponde a tu función deberán ser reportados a tu jefe inmediato. Tener en cuenta que los accesos que no corresponden a tu perfil, no hacer el uso de ellos, ni mucho menos probar las debilidades de los sistemas informáticos.

5

Ley N° 297333 de Protección de Datos Personales

El objetivo de la Ley N° 29733 es velar por el derecho fundamental a la protección de datos personales, a través de su adecuado tratamiento, esta ley es aplicable y de cumplimiento obligatorio para todas las empresas y se aplica a todas las áreas de la empresa que mantengan un banco de Datos Personales.

¿Qué son los datos personales?

Es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. A continuación, se mencionan algunos datos personales que identifican o hacen identificables a una persona física:

- Datos de Identificación: DNI, pasaporte, domicilio, teléfono, email.
- Datos de características personales: estado civil, nacionalidad, profesión.
- Datos de características social: pasatiempo, perteneciente a un club.

¿Qué son los Datos Sensibles?

Es cualquier información que afecta la esfera más íntima de la persona, y su divulgación indebida puede ocasionar daño al honor y a la intimidad de la persona. Por lo tanto, se requiere mayor protección y tratamiento especial de acuerdo con la ley que lo establece.

Algunos datos sensibles son:

- Datos raciales y étnicos.
- Ingresos económicos.
- Opciones Políticas, religiosas, filosóficos o morales.
- Afiliación sindical.
- Información relacionada a la salud o a la vida sexual.

¿Qué es el tratamiento de datos personales?

Si la organización solicita información personal de clientes, colaboradores o terceros, ya sea de forma automatizada (a través de medios tecnológicos) o no automatizada y, además, recopila, almacena, conserva, o registra, se está realizando tratamiento de datos personales y por ende se deberá cumplir con lo que dispone la Ley de Protección de datos personales.

¿Qué es un Banco de Datos Personales?

Es el conjunto organizado de datos personales, automatizado o no, independiente del soporte en el cual sea contenido (Impreso, digital, óptico, etc.) que se mantenga en la empresa. Generalmente, los bancos de datos personales que se encuentran en una empresa son de los trabajadores, clientes, proveedores, postulantes, entre otros. La Ley de Protección de Datos aplica a datos personales contenidos o destinados a ser contenidos en bancos de datos personales privados o públicos.

¿Qué son mis derechos ARCO?

Son un conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales, y son:

Derecho de Acceso: Averiguar si tus datos personales están disponibles para tratamiento en el banco de datos de cualquier empresa y con qué fines son usados.

Derecho de Rectificación: Actualizar o completar los datos personales faltantes, erróneos o falsos.

Derecho de Cancelación: Solicitar la eliminación de tus datos personales del banco de datos de la empresa cuando estos hayan dejado de ser necesarios para la finalidad brindada.

Derecho de Oposición: Solicitar la eliminación de tus datos personales del banco de datos de la empresa cuando estos hayan dejado de ser necesarios para la finalidad brindada.

¿Dónde puedo leer información sobre el proceso disciplinario o en qué documento de Conexa se encuentra?

En nuestra sección de documentos en BUK y también es enviado mediante correo electrónico desde el área de Recursos Humanos a todos los colaboradores.