



**CORREDOR
EMPRESARIAL**
S.A



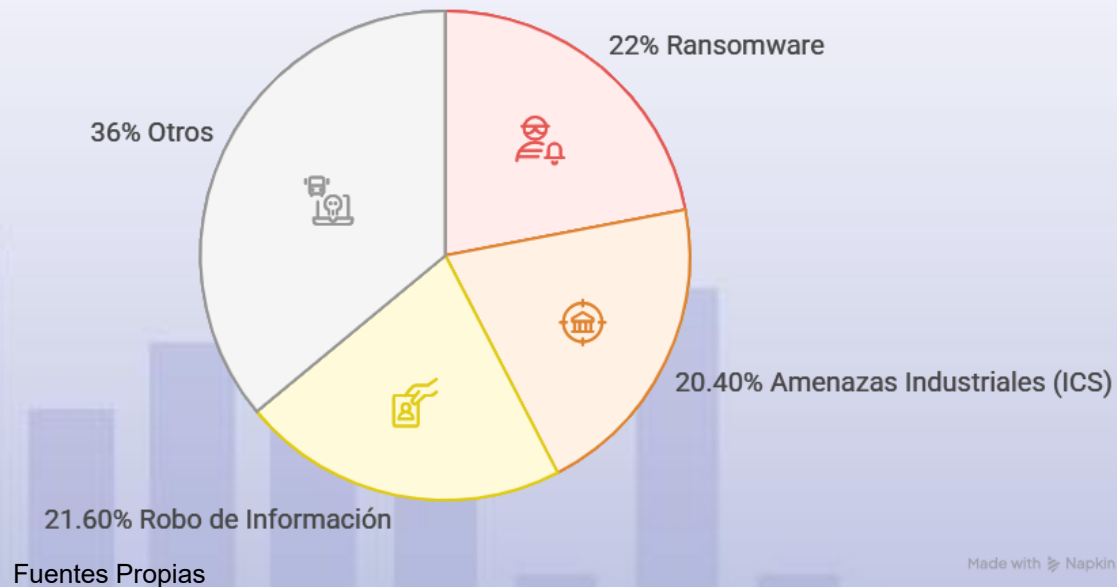
Inducción Seguridad de la Información

Antecedentes y Contexto de Seguridad Informática

Un reporte del Índice de Inteligencia de Amenazas X-Force de IBM 2025, ubica a Colombia como el primer país en Latinoamérica con mayor número de ciberataques.



Distribución de Amenazas Cibernéticas



108%
Aumento en
ataques
cibernéticos

54.000
millones
Ciberataques
en Colombia

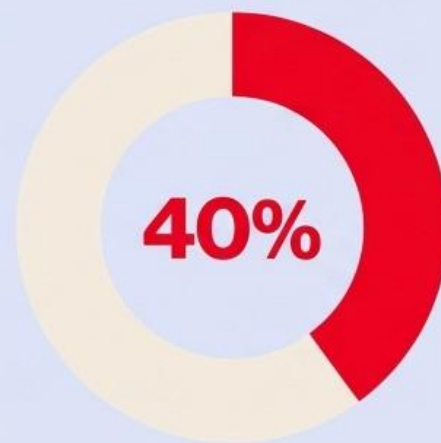
Antecedentes y Contexto de Seguridad Informática

La ciberseguridad es un deporte de equipo.



Las violaciones con participación de terceros han aumentado un 60% desde el año pasado y ahora representan el 48% de las violaciones,² resaltando lo crucial que es vetar —y colaborar con— sus socios.

Cuando estás en tu teléfono, los tipos malos van de pesca (phishing).

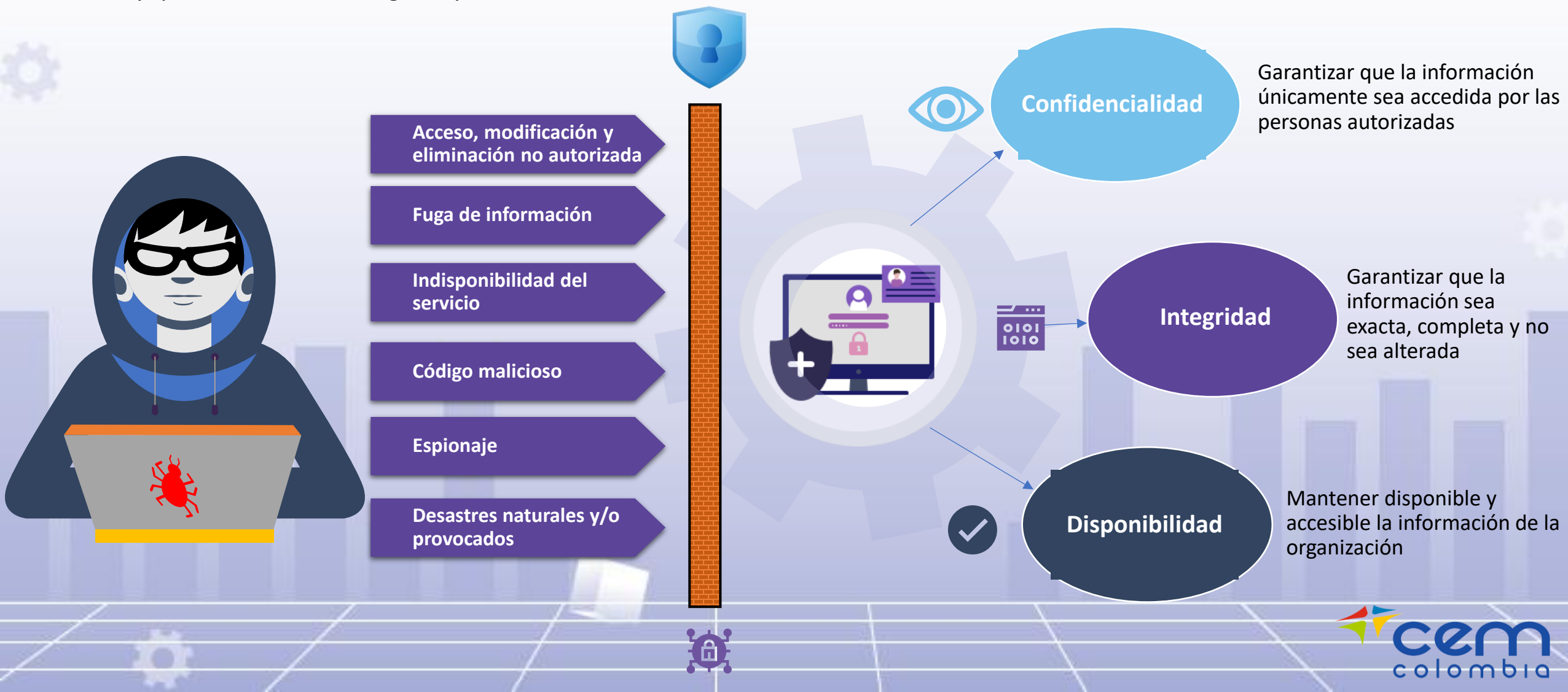


En simulaciones de phishing, los ataques con puntos de entrada basados en móviles (p. ej., voz y texto) tuvieron una tasa mediana de clics exitosos un 40% más alta que los que entraban por correo.

Informe de investigaciones sobre violaciones de datos

¿Por qué de la Seguridad de la Información?

Porque protege la confidencialidad, integridad y disponibilidad de la información, asegurando que solo personas autorizadas tengan acceso y que los datos estén seguros y accesibles cuando se necesiten.



4.1-RESPONSABILIDADES - OBLIGACIONES COLJUEGOS

Coljuegos nos autoriza para la operación de nuestros diferentes productos a través de las siguiente Normativa:



- BetPlay: Contrato C1876 de 2022
- SUPERastro: Contrato 2157 de 2025
- Chance Millonario: Acuerdo 326 de 2017



Por medio de esta normativa, nuestras obligaciones generales como empleados de Corredor Empresarial S.A. son las siguientes:

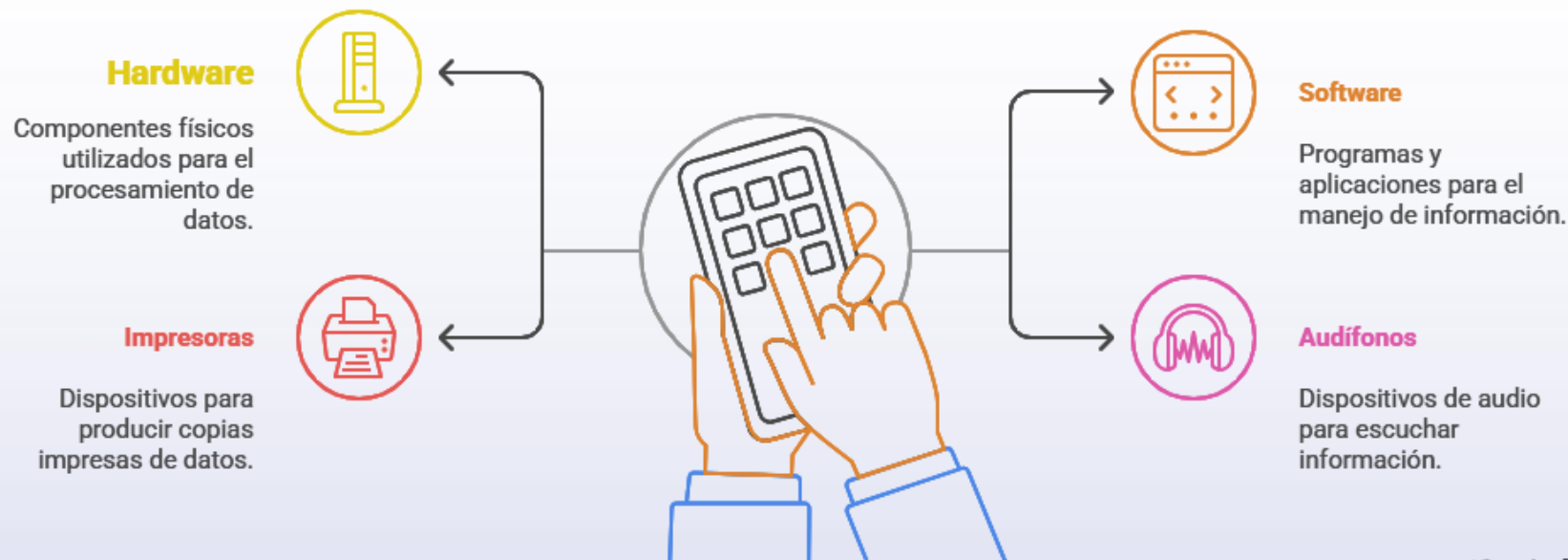


- ✓ Garantizar la disponibilidad y operatividad de los sistemas de juego
- ✓ No difundir información confidencial, debilidades o amenazas de los sistemas de juego o de los procesos de la compañía.
- ✓ Velar por el cumplimiento de las normas sobre prevención de lavado de activos.
- ✓ Responder oportunamente toda petición, queja o reclamo que generen los jugadores o partes interesadas.
- ✓ Verificar la información brindada por el jugador.
- ✓ Garantizar el cumplimiento de las restricciones de juego (menores de edad, enfermos mentales o personal empleado).
- ✓ Tener controles técnicos o de procesos para evitar posibles fraudes.
- ✓ Reportar a los canales corporativos sobre cualquier evento o incidente de seguridad.
- ✓ Permitir el acceso a Coljuegos para el control y revisión de los sistemas de juego.

Dispositivos Móviles, Teletrabajo y Trabajo en Casa



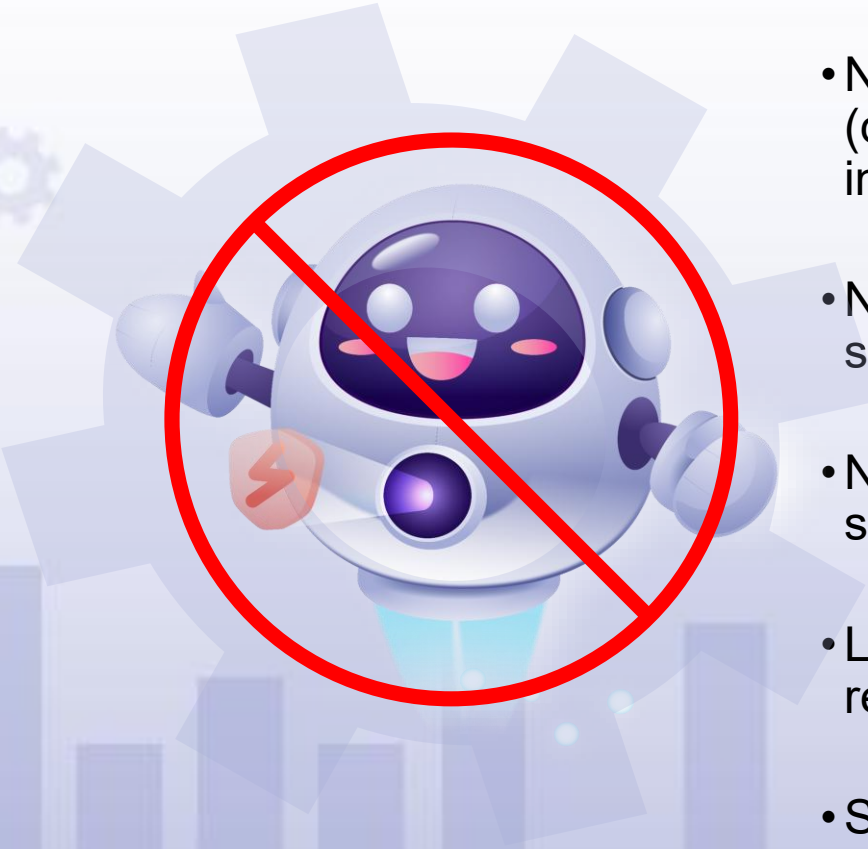
Manejo de Activos de Información



- **Clasificación o etiquetado** de la información debe realizarse por el líder de proceso propietario del activo, quien es el responsable de mantenerla actualizada a lo largo de su ciclo de vida.



- Tener procedimientos para acceso físico y de videovigilancia a directivos, empleados, visitantes, contratistas y proveedores a las instalaciones en coordinación con la Gerencia Administrativa, Seguridad de la información y el área de Tecnología e Infraestructura.
- Los accesos deben ser solicitados y autorizados por el Gerente o Director de proceso al área de Tecnología la cual debe generar un ticket.
- El empleado es responsable de sus credenciales y debe asumir la responsabilidad del acceso otorgado asegurando el uso adecuado de este.
- Es responsabilidad de cada Gerencia o área dueña de proceso, el mantenimiento de los roles y privilegios configurados o asignados a los diferentes activos de información por medio de la SIGO-SI-13.2-IA-FR Matriz de Roles y Privilegios, esta revisión se recertificará semestralmente.
- El líder de proceso con la colaboración del proceso de Talento Humano, deberán gestionar la baja de los identificadores de los empleados propios que hayan terminado su relación laboral con la empresa.
- Utilizar contraseñas robustas seguras y cambiarlas frecuentemente o cuando se sospeche que han sido comprometidas.



- No se permite que varios usuarios compartan el mismo identificador (denominados usuarios genéricos) en la red o diferentes sistemas de información de Corredor Empresarial S.A.
- No compartir las credenciales de acceso asignadas a los diferentes sistemas o aplicaciones.
- No utilizar los usuarios o contraseñas que vienen por defecto en los sistemas de información.
- Las credenciales de acceso No deben ser escritas, copiadas o reproducidas en papel o en un documento electrónico sin protección.
- Se prohíbe la conexión de dispositivos de almacenamiento externos, tales como memorias USB, dispositivos de almacenamiento extraíbles y discos duros portátiles.



- Impedir la conexión directa de entrada o salida de tráfico entre Internet y las redes de la Compañía.
- Habilitar sólo servicios y protocolos seguros que sean necesarios según lo requiera la función del sistema.
- El acceso a la red por parte de Visitantes (Clientes, Proveedores y cualquier personal externo) en la compañía, sólo está autorizado por medio de la red inalámbrica creada para tal fin.
- La conexión remota a la red de área local de Corredor Empresarial S.A, debe realizarse a través de una conexión segura.
- Es responsabilidad del área o dueño del proceso informar al área de Tecnología e Infraestructura, para realizar la desactivación o renovación de los servicios de conexión de terceros.
- No está autorizado el uso o implementación de redes inalámbricas independientes (Router, Modems o de tipo AD HOC), entre dispositivos que puedan acceder a la información o a las redes internas de la compañía.

Escritorio y Pantalla Limpios

Para mantener la confidencialidad, integridad y disponibilidad de la información, los empleados deberán mantener buenas prácticas de seguridad en su puesto de trabajo:

- En el momento de la asignación de un activo, el empleado se convierte en su custodio y responsable.
- Guardar bajo llave la información sensible en papel o almacenada en soportes digitales.
- Bloquear la sesión de trabajo del equipo de cómputo al ausentarse del puesto de trabajo.
- No navegar por sitios no confiables o que puedan facilitar la propagación de virus y/o spam, descargar y/o instalar software o material protegido con las restricciones de propiedad intelectual sin la correspondiente licencia de uso, intercambiar información sensible sin una protección adecuada, etc.
- No publicar información de la empresa (documentos, videos, opiniones, etc.) sin autorización en servidores públicos de Internet.



Respaldo de Información

El área de Tecnología e Infraestructura definirá los programas de respaldo de información con tiempos de retención. Las retenciones adicionales a las definidas deberán ser confirmadas al área de Tecnología por los líderes de los procesos de la compañía.

Todas las copias de seguridad de la información Reservada o Confidencial deben ser almacenadas en un área aprobada con acceso controlado y condiciones ambientales adecuadas que garanticen su preservación.

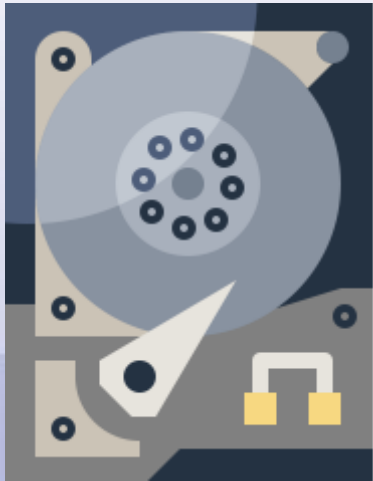
Las copias de respaldo deben ser custodiadas en una instalación diferente al sitio de procesamiento de la información, con el fin de garantizar la continuidad del negocio.

- Es necesario que los medios magnéticos y ópticos sean correctamente etiquetados y organizados para facilitar su identificación y ubicación en el momento en que se requiera recuperar información.
- El área de Tecnología e Infraestructura debe documentar los procesos de ejecución de restauraciones de copias de seguridad para cada tipo de información a respaldar.



Eliminación de Información

Las solicitudes de destrucción o eliminación de información pueden generarse desde las áreas internas de Corredor Empresarial S.A. o por parte de sus clientes.



- La información propia de la compañía, sólo se podrá eliminar o destruir con autorización previa del Gerente o director de área y la validación del dueño del proceso y que no vaya en contravía de la normatividad vigente o acuerdos contractuales con partes interesadas.



Seguridad Física

La seguridad física protege a las personas, instalaciones y activos contra amenazas físicas, asegurando la integridad y continuidad operativa.



- Es obligatorio registrar el ingreso y la salida mediante el sistema biométrico de acceso.
- Informar inmediatamente sobre cualquier actividad o persona sospechosa
- No divulgar información confidencial o sensible.
- Respetar las políticas de no acceso a áreas restringidas sin autorización.
- Respetar las políticas y normas de acceso de visitantes.
- No dejar dispositivos electrónicos desatendidos.
- Bloqueo de equipos de cómputo cuando no estén en uso.
- No conectar dispositivos USB desconocidos a las computadoras de la empresa.

Anonimización de datos



La anonimización es el proceso de eliminar o modificar información personal identificable de un conjunto de datos, de manera que las personas a las que se refiere no puedan ser identificadas directa o indirectamente.

Enmascarado de datos (blacklining)

First name	Last name	CC number
Denise	Smith	5248 6842 2178 3954
Monica	Hanraets	5830 8506 1640 3677
Youri	Soler	3226 4901 4892 9975
Stella	Montagna	9757 6035 3687 6841
Hamlet	Donnelly	6901 0354 6872 9865
Soraya	Lachance	1778 6983 2647 3205

First name	Last name	CC number
Denise	Smith	██████████ 3954
Monica	Hanraets	██████████ 3677
Youri	Soler	██████████ 9975
Stella	Montagna	██████████ 6841
Hamlet	Donnelly	██████████ 9865
Soraya	Lachance	██████████ 3205



Anulación (borrado)

First name	Last name	Middle name
Denise	Smith	Joanna
Monica	Hanraets	Elena
Youri	Soler	Michael
Stella	Montagna	Valerie
Hamlet	Donnelly	René
Soraya	Lachance	Violet

First name	Last name	Middle name
Denise	Smith	NULL
Monica	Hanraets	NULL
Youri	Soler	NULL
Stella	Montagna	NULL
Hamlet	Donnelly	NULL
Soraya	Lachance	NULL

Encriptación de datos

First name	Last name	CC number
Denise	Smith	5248 6842 2178 3954
Monica	Hanraets	5830 8506 1640 3677
Youri	Soler	3226 4901 4892 9975
Stella	Montagna	9757 6035 3687 6841
Hamlet	Donnelly	6901 0354 6872 9865
Soraya	Lachance	1778 6983 2647 3205

First name	Last name	CC number
Denise	Smith	0?nfaZ&-002#a\$/@¶ñ
Monica	Hanraets	Bg6l»¥e\$QJâ<¼¢πÛa
Youri	Soler	j!+K4LÉÁ\$ffTh00;Piq!
Stella	Montagna	úJf6* "C=√vŴG@0ēz2
Hamlet	Donnelly	h=¼5Dgēl~RijÅg{«™Üē-
Soraya	Lachance	3Y@>µubGâk^,tTÖc4}

Olivia Wilson
MUSIC TEACHER

📞 +123-456-7890
✉️ hello@realtygreatsite.com
🌐 www.realtygreatsite.com
📍 123 Anywhere St., Any City, ST 12345
📅 Date of birth: 13-09-1981

About Me

A positive and motivated individual committed to excellence and successful outcomes. A dedicated and focused teacher who excels at prioritizing, completing multiple tasks simultaneously, and following through to achieve project goals.

Skill

- Communication skills
- Collaboration
- Instructional skills
- Classroom management
- Listening skills
- Personableness
- Knowledge of musical elements
- Knowledge of recording equipment

Career

Private Music Tutor
October 2006- June 2013

- Develop lesson plans and instructional materials.
- Taught individual music lessons to students.
- Designed personal website for the purpose of marketing.

Music Teacher
August 2015-present

- Creates engaging lesson plans and integrates educational technology to drive retention, comprehension, and participation. Accomplished in building trust and meaningful relationships between students, parents, and administrators.

Education

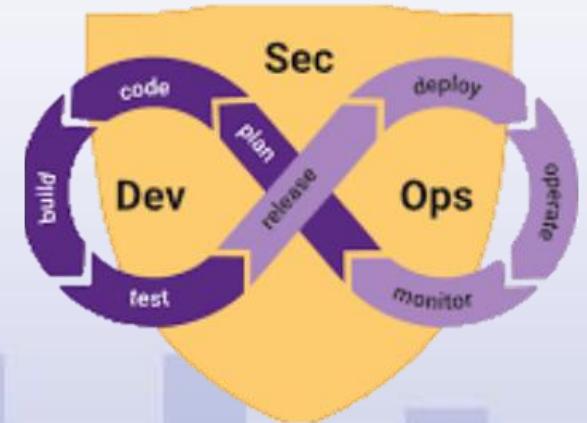
Master of Music
University of Music, 2015, London



El área de Tecnología y Desarrollo establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.

- Se debe contar con ambientes independientes de Desarrollo, Pruebas y Producción para el desarrollo de software, estos deben contemplar controles físicos y de acceso lógico para garantizar la separación de los mismos.
- Utilizar cuentas de usuario diferentes para los ambientes de desarrollo, pruebas, y producción (las mismas deben cumplir con los criterios del uso adecuado de contraseñas).
- Desarrollos inventariados, plenamente documentados y registrados legalmente.
- Se debe restringir y auditar el acceso a los repositorios del código fuente de los desarrollos.

DevSecOps



Como parte de las actividades del ciclo de vida del desarrollo se deben tomar como referencia, prácticas reconocidas de codificación segura (ejemplo: OWASP, NIST 800, SANS CWE Top 25, CERT Secure Coding, etc).

Inspecciones de Seguridad de la Información



El objetivo de las inspecciones de Seguridad de la Información es el de validar con los diferentes procesos de Corredor Empresarial S.A., la aplicación de las políticas y normatividad interna; también identificar nuevos riesgos, vulnerabilidades o incidentes relacionados con la Seguridad de la Información.



Las áreas técnicas y de control de Corredor Empresarial S.A. podrán realizar las siguientes actividades para validar el estado del cumplimiento de lo emanado por seguridad de la información:

- **Auditorias de cumplimiento o periódicas bajo el estándar ISO 27001:2022 que se debe realizar mínimo una vez al año para la verificación del estado del cumplimiento.** Las auditorias serán realizadas por auditores internos o externos según aplique.
- **Test de Penetración o pruebas de Ethical Hacking** como validación de las medidas de seguridad de la información en la infraestructura tecnológica de la compañía, los cuáles serán ejecutadas por un tercero, quien generará el informe correspondiente para que se establezca el plan de remediación.
- **El área de Tecnología debe realizar revisiones periódicas** para verificar que los sistemas de información cumplan con lo emanado por seguridad de la información.

Es responsabilidad de los dueños o líderes de procesos realizar seguimiento a las acciones correctivas, preventivas y planes de remediación que puedan ser generados como resultado de estas inspecciones y pruebas aplicadas.

Incidentes de Seguridad de la Información

Todos los empleados de Corredor Empresarial S.A., son responsables de reportar debilidades, eventos e incidentes de Seguridad de Información de los cuales tengan conocimiento en las plataformas, activos de información digitales o los mismos activos de información físicos que estén bajo su cargo.

- Se establece un **Equipo de Gestión de Incidentes** de seguridad de la compañía que estará conformado como mínimo por:

- ✓ El propietario y/o custodio del activo
- ✓ El profesional o equipo de la gerencia de Tecnología que apoya la gestión de incidentes de seguridad
- ✓ El Oficial de Seguridad de la Información
- ✓ Demás profesionales de las áreas de la compañía que tengan a cargo activos o procesos que se vean afectados por el incidente
- ✓ Además el profesional de la gerencia Oficial de Cumplimiento que participará si se ve afectada una base de datos con datos personales o información sensible.

- El Equipo de Gestión a incidentes podrá solicitar la participación de otros empleados, procesos, especialistas y/o terceros requeridos para la atención del incidente de seguridad.

ATAQUES RELEVANTES A EMPRESAS Y GOBIERNOS 2025-2026				
Casos reales que demuestran que ningún sector está exento. La ciberseguridad es responsabilidad de todos.				
FECHA	ORGANIZACIÓN / PAÍS	¿QUÉ PASÓ?	IMPACTO PRINCIPAL	LECCIÓN CLAVE
7 AGOSTO 2026	Levi Strauss (Global)	La empresa informó un incidente de ciberseguridad relacionado con ingeniería social dirigida contra tres empleados.	Posible acceso no autorizado a información corporativa. Investigación en curso.	Los atacantes pueden engañar a las personas para obtener acceso.
JULIO 2026	Ecopetrol (Colombia)	Un ciberataque comprometió información relacionada con aprox. 3.300 cuentas de usuarios almacenadas en servicios cloud.	Riesgo de exposición de datos y extorsión. El atacante intentó realizar exigencias económicas.	La información en la nube también debe estar protegida y monitoreada.
6 MARZO 2026	DIAN (Colombia)	Ataque al sistema de agendamiento de citas de un proveedor tecnológico. Acceso no autorizado a datos personales de ciudadanos.	Exposición de datos personales. La información tributaria y credenciales no fueron comprometidas.	Los proveedores y terceros también pueden ser puertas de entrada.
7 AGOSTO 2026	Suisun City (California, EE. UU.)	Ataque que obligó a apagar la red informática de la ciudad y afectó servicios públicos, incluyendo parte del 911.	Interrupción de servicios críticos y atención a emergencias.	Los ataques pueden afectar servicios críticos y poner vidas en riesgo.
SEPTIEMBRE 2025	Jaguar Land Rover (Reino Unido)	Ciberataque que obligó a apagar sistemas y provocó una interrupción severa de producción y ventas durante varias semanas.	Pérdidas millonarias, afectación a proveedores, clientes y cadena de suministro.	Un ataque puede detener la operación completa de una empresa.
SEPTIEMBRE 2025	M&S (Reino Unido)	Ransomware que afectó sistemas corporativos, operaciones en línea y tiendas físicas.	Impacto en ventas, operación y datos de clientes.	El ransomware puede afectar todo el negocio, no solo la tecnología.
SEPTIEMBRE 2025	Co-op Group (Reino Unido)	Ciberataque que afectó sistemas de TI y disponibilidad en tiendas por varios días.	Interrupción de operaciones y costos de recuperación.	La detección temprana y los planes de respuesta reducen el impacto.
2025 (Varias fechas)	Entidades públicas y empresas (Colombia)	ColCERT reportó múltiples campañas de phishing, ransomware y robo de información dirigidas a sectores estratégicos del país.	Robo de credenciales, exfiltración de información y posibles extorsiones.	Los atacantes siempre buscan aprovechar vulnerabilidades y el factor humano.

Gracias