POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

Intercorp Retail

InRetail Perú adoptó la Política Corporativa de Seguridad de la Información de Intercorp Retail.

Actualización aprobada en Directorio del 27 de agosto de 2026.

1. OBJETIVO

Establecer políticas que permitan mantener la confidencialidad, integridad y disponibilidad de la información y recursos de las Unidades de Negocio (UN) y de la Unidad Corporativa (UC) que forman parte de Intercorp Retail e InRetail Perú Corp.

2. ALCANCE

Esta política aplica a la Unidad Corporativa (UC) y a todas las Unidades de Negocio (UN) de Intercorp Retail e InRetail Perú Corp. y las que pudiese tener en el futuro.

3. DEFINICIONES

3.1. **Activos de información:** Todo aquello que tenga valor para la UN como, por ejemplo: Información electrónica y física, Software, Hardware, Red de datos, Personas, Servicios.

3.2. **Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso**.**

3.3. **Colaborador:** Aquella persona que presta un servicio determinado dentro de las instalaciones de la UN a cambio de una remuneración.

3.4. **Confidencialidad:** Característica de la información por la cual ésta es de conocimiento y uso reservado sólo para algunas personas, por lo que no será divulgada a personas, entidades o procesos no autorizados, ni utilizada para fines no autorizados. Los datos personales son una modalidad de información confidencial.

3.5. **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

3.6. **Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

3.7. **Equipos móviles:** Dispositivos electrónicos portátiles como laptop, tablet, celular, etc.

3.8. **Home Office (VPN):** Portal que brinda acceso remoto al equipo del colaborador para administrar información y/o recursos.

3.9. **Internet:** Red mundial de comunicaciones que interconecta redes académicas, corporativas y comerciales.

3.10. **Proveedor:** Persona o empresa externa responsable de suministrar bienes o servicios a la UN por períodos.

3.11. **Recursos Informáticos:** Son las aplicaciones (software) y equipos informáticos (hardware).

3.12. **Servicios Ofimáticos:** Se refiere a los servicios de las fotocopiadoras, impresoras y escáneres para la optimización de la gestión de documentos en oficinas.

3.13. **Servicios en Red:** Son aquellos servicios como el acceso a la red interna, mensajería instantánea, internet o directorios.

3.14. **Spam:** Envío o recepción masiva de mensajes de correo no autorizado o no solicitado.

3.15. **Titular de datos personales:** Persona natural a quien corresponde los datos personales.

3.16. **Tratamiento de datos personales:** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación, entrega o interconexión de los datos personales.

3.17. **Disponibilidad:** Característica de la información que hace referencia a que pueda ser accedida y utilizada cuando sea requerida

3.18. **Integridad:** Es la característica de la información que hace referencia a la exactitud y fiabilidad. La integridad de la información tiene como objetivo evitar modificaciones, alteraciones o destrucciones no autorizadas.

3.19. **Privacidad:** Se refiere al derecho de mantener la confidencialidad de la información, es decir de salvaguardar y proteger información contra el acceso no autorizado.

4. RESPONSABILIDADES DEL PROVEEDOR DE SERVICIOS

4.1. El/La Head de Ciberseguridad es responsable que la presente política se comunique, se cumpla y refleje la visión de Intercorp Retail.

4.2. Todos los colaboradores de las UNs y de la UC son responsables de cumplir y hacer cumplir la presente política.

5. LINEAMIENTOS DE LA POLÍTICA

5.1. Generales

- Todo dato contenido en un activo de la información es propiedad de las UNs y, por lo tanto, debe protegerse, mantenerse y gestionarse adecuadamente para que no sea alterada o destruida de forma inadecuada.

- Los sistemas de información de la compañía contienen información patentada y pueden contener información confidencial. Por lo tanto, todos los usuarios son responsables de

garantizar que los datos, la información y los recursos informáticos se utilicen única, exclusiva y directamente para respaldar las prácticas y negocios de la compañía.

- Todos los dispositivos utilizados para proteger, mantener la integridad, disponibilidad y confidencialidad de la información deben considerarse información privada, por lo que está prohibida su divulgación a personas no autorizadas (empleados o terceros).

- Los colaboradores están obligados a mantener en reserva todo documento, información o material que es considerado como información confidencial de la UC o la UN. En tal sentido, no podrán publicar, usar, disponer para sí o para terceros, comercializar, ceder, vender, compartir, donar o realizar cualquier otra forma de transferencia a favor de terceros, ningún documento, información, instrumento, aportes, adquisiciones o conocimientos que se señalan a continuación: base de datos en general, datos personales, desarrollo de software, proyectos, estrategias, indicadores de gestión, información relativa a ventas, compras, costos, negociaciones, socios estratégicos, proveedores, colaboradores, clientes, y demás información de similar naturaleza.

- Sólo podrán tener acceso a la información referida en el párrafo anterior aquellos colaboradores que resulten indispensables para el cumplimiento de los fines de que se trate en cada caso. Dichos colaboradores deberán utilizar la información única y exclusivamente para tales fines.

- Los conocimientos, aportes y/o tecnologías desarrolladas durante la vinculación laboral del colaborador quedan como patrimonio exclusivo de la UN.

- Los responsables de la información en coordinación con Seguridad de la Información o su equivalente deben definir mecanismos que garanticen la integridad, disponibilidad, seguridad frente a accesos no autorizados, y confidencialidad de la información.

5.2. Gobierno de Seguridad de Información

El Gobierno de Seguridad de Información y/o Ciberseguridad contempla la siguiente estructura a nivel corporativo y a nivel unidad de negocio:

5.2.1 A nivel UC:

- CISO: El rol de CISO (Chief Information Security Officer) recaerá sobre el cargo de Head de Ciberseguridad de Intercorp Retail con la responsabilidad corporativa de la seguridad de la información. Sus principales responsabilidades se relacionarán:
  - Definir el plan estratégico corporativo de seguridad de información y ciberseguridad para el control o mitigación de riesgos de seguridad de información con impacto crítico en las operaciones de las UNs.
  - Supervisar y asesorar al rol de BUISO en el desempeño de sus responsabilidades.
  - Entregar informes periódicos, con indicadores a la Vicepresidencia de TI y Gerencias Generales relacionadas.

5.2.2 A nivel UN:

- BUISO: El rol de BUISO (Business Unit Information Security Officer) recaerá sobre el cargo de Gerente, Jefe, Supervisor de Seguridad de Información o sus semejantes en la UN. Sus principales responsabilidades se relacionarán:
  - Ejecutar y complementar el plan estratégico corporativo de seguridad de información y ciberseguridad para el control o mitigación de riesgos de seguridad de información con impacto crítico en su UN.
  - Realizar el análisis de riesgos de ciberseguridad o seguridad de información para determinar la exposición al riesgo de su UN.
  - La auditoría de seguridad, y de ser el caso, la revisión de planes de acción de seguridad.
  - Entregar informes periódicos, con KRIs y KPIs a la Dirección o Gerencia de TI de su UN.

5.3. Continuidad Operativa

- Los entornos de procesamiento y transmisión de datos proporcionados por la UN deben contar con planes de contingencia y recuperación que deben ser revisados y probados periódicamente.

- Las Vicepresidencias, Gerencias y/o Direcciones de las UNs deberán designar un dueño por aplicación el cual deberá de definir y exigir los tiempos de recuperación necesarios para la continuidad operativa de sus procesos operativos al área de TI, Sistemas o su equivalente.

5.4. Adquisición de tecnologías de información y contratos con terceros:

- Todos los acuerdos con terceros deben estar aprobados técnica y comercialmente cumpliendo con los estándares de seguridad de la compañía aprobados por el área de Ciberseguridad, Seguridad de Información o sus semejantes.

- Cualquier proceso de adquisición y/o contratación de proveedores de activos y/o servicios deberá guiarse por los siguientes lineamientos referenciados en la Política de Seguridad para Proveedores:

  - El acceso a cualquier información propiedad de la compañía deberá otorgarse al proveedor sólo después de la formalización y firma de un "Acuerdo de Confidencialidad" y/o Contrato.
  - El acceso a los recursos tecnológicos y sistemas de información se asignará individualmente al proveedor tras la formalización y firma de un “Acuerdo de Confidencialidad” y/o Contrato.
  - En caso el contrato tenga una relación directa con riesgos de seguridad de información, que puedan poner en perjuicio la confidencialidad, integridad y disponibilidad de la información de la compañía, se debe de contar con la aprobación del Head, Gerente o Líder de Seguridad de Información de la UN.

- Gerente o Líder de Seguridad de Información de la UN deberá de evaluar los riesgos de seguridad de información relacionados y exigir los controles mitigatorios de reducción para la aceptación del servicio. Por ejemplo: Ciberseguros, cláusulas de responsabilidad ante impactos financieros por ciber incidentes materializados, certificaciones y estándares globales de seguridad, resultados periódicos de auditorías de Ciberseguridad, entre otros.

5.5. Seguridad física y ambiental

- Todos los colaboradores deben usar una identificación visible. Se debe notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado.

- Los colaboradores a los que se les haya asignado una laptop deberán mantenerla con el cable de seguridad mientras permanezcan en las oficinas, siendo responsables de resguardar la seguridad de los activos tecnológicos asignados.

- Los colaboradores que vengan a trabajar fuera de horario de oficina, fin de semana o feriados deberán ser registrados.

- Los colaboradores responsables de mantener servicios con personal tercero como proveedores deberán comunicarse con el agente de seguridad o recepción de turno a fin de que facilite el ingreso en horario de oficina.

- Todo documento físico con datos personales deberá ser almacenado en armarios, archivadores u otros elementos ubicados en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

- Deberá existir una lista de personal autorizado a tener acceso frecuente a las áreas donde se almacenen documentos físicos con datos personales; todo acceso distinto al autorizado será registrado indicando al menos los siguientes campos:
  - Persona que tuvo acceso a la información
  - Motivo de acceso
  - Fecha y hora de acceso
  - Datos personales consultados

5.6. Accesos y credenciales

- Las credenciales de acceso a los recursos informáticos son personales e intransferibles y sólo deberán ser utilizadas en el equipo asignado al colaborador responsable de la cuenta.

- En caso de que el colaborador tenga algún inconveniente con sus accesos no deberá revelar sus contraseñas, ya que los especialistas deben realizar descartes con el apoyo del colaborador o con sus credenciales de administrador.

- Toda acción hecha con las credenciales (usuario y contraseña) serán solo responsabilidad del propietario de la cuenta, por lo tanto, queda prohibido el uso de las credenciales de otro colaborador.

- El colaborador deberá elegir una contraseña para el acceso a los sistemas y recursos informáticos.

- Se recomienda utilizar contraseñas robustas, combinaciones de 8 o más caracteres alfabéticos, números y símbolos (por ejemplo: '$3gurid4d') y evitar utilizar contraseñas que sean solo palabras o números con algún significado (nombres, ciudades, fecha de nacimiento, DNI, teléfono u otro relacionado), para las aplicaciones en las que corresponda.

- El desbloqueo deberá ser solicitado únicamente por el propietario de la cuenta o Responsable de su área a Centro de Servicios, identificándose previamente.

- Los colaboradores no deben permitir que otra persona utilice las computadoras que se les ha asignado, salvo que supervisen el uso de su computadora cuando se acepte que el personal de Soporte TI o su equivalente, debidamente autorizado, acceda física o remotamente al equipo.

- La creación y modificación de accesos a los servicios de red y recursos informáticos deben ser solicitados por personal autorizado al Centro de Servicios o su equivalente, incluyendo sus datos, los cuales serán asignados de acuerdo con su cargo o aprobación.

- El acceso de proveedores o invitados a la red y servicios de la UN debe ser solicitado por un colaborador interno como responsable al Centro de Servicios o su equivalente incluyendo el motivo, los niveles de privilegios y periodo de validez.

- Todas las cuentas con tiempo de inactividad mayor a 90 días serán eliminadas. Toda excepción deberá ser notificada a Seguridad de la Información o su equivalente especificando el motivo y aprobación del responsable del área. La reactivación tendrá el mismo procedimiento de una creación.

- Todas las cuentas de personal cesado serán desactivadas y/o eliminadas. Toda excepción deberá ser notificada anticipadamente a Seguridad de la Información o su equivalente especificando el motivo, periodo de validez y aprobación del responsable del área.

- La UN se reserva el derecho de revocar, a cualquier usuario, los privilegios de acceso a los sistemas, cuando la UN lo considere pertinente.

- Los colaboradores deben reportar los inconvenientes e incidencias de accesos a los recursos informáticos a Centro de Servicios o su equivalente.

- Queda prohibida la recopilación, almacenamiento, tratamiento o entrega de datos personales de los clientes y/o clientes prospecto de la UN sin la autorización de la Gerencia Comercial o equivalente.

- Queda prohibida la recopilación, almacenamiento, tratamiento o entrega de datos personales de los colaboradores y postulantes de la UN sin la autorización de la Gestión de Desarrollo Humano o su equivalente.

- Queda prohibida la recopilación, almacenamiento, tratamiento o entrega de datos personales de los proveedores personas naturales de la UN sin la autorización de la Gerencia de Finanzas o equivalente.

- Queda prohibida la recopilación, almacenamiento, tratamiento o entrega de datos personales obtenido a través del sistema de video vigilancia de la UN sin la autorización de la Gerencia de Administración y Operaciones o su equivalente.

5.7. Uso aceptable

Los colaboradores y terceros que presenten servicios para la UC y/o UNs, deberán de aceptar y seguir los lineamientos definidos en el documento *"Política Corporativa de uso Aceptable de Activos"*, de la cual los principales lineamientos de seguridad son:

5.7.1 Uso y protección de recursos informáticos y activos

- En caso de que los colaboradores necesiten un software y/o hardware, el responsable de su área deberá formalizar el pedido ante el Centro de Servicios o su equivalente. Toda solicitud de software nuevo debe ser analizada por el área de Soporte TI o su equivalente y autorizado por Seguridad de la Información o su equivalente.

- Los colaboradores no deben ejecutar, utilizar e instalar software proveniente de fuentes no confiables, sin licenciamiento corporativo o de distribución gratuita, incluyendo el que haya sido adquirido por el propio colaborador, esto es con el fin de prevenir demandas legales o introducción de virus informáticos.

- Los colaboradores solo deberán utilizar para fines laborales los recursos informáticos asignados por la UN.

- Los colaboradores deben asumir que todo el software de la UN está protegido por derechos de autor y requiere licencia de uso, por lo cual no está permitido copiar, transferir, divulgar o instalar el software a otra computadora.

- Los colaboradores que necesiten utilizar algún dispositivo móvil personal conectado a la red interna deberán ser aprobados por Seguridad de la Información o su equivalente y revisado por Soporte TI, quienes aplicarán las políticas de las UN previo ingreso a la red.

- Para movilizar los activos de Sistemas de la UN, dentro de la misma sede, se deberá contar con la aprobación del responsable del área origen y destino, además de solicitar apoyo al personal correspondiente. En caso de ser un traslado fuera de las instalaciones de la UN, deberá ser coordinado con el área de Sistemas o su equivalente y contar con una guía de remisión aprobada.

- El acceso a los repositorios web únicamente es autorizado a los recursos licenciados por la compañía. Se encuentra restringida la carga de información de la UC o UN en repositorios web públicos.

- El intercambio de datos personales y demás información confidencial hacia cualquier destino fuera de las instalaciones físicas de la UN, dentro o fuera del territorio nacional, solo procederá con la autorización del responsable del área y se hará utilizando los medios de transporte autorizados por el mismo, tomando las medidas necesarias con el fin de evitar el acceso no autorizado, pérdida o corrupción durante el traslado hacia su destino. El transporte electrónico de datos se realizará mediante protocolos seguros cifrados.

- Los colaboradores deberán solicitar, en forma oportuna, al área de Soporte TI la eliminación de los medios informáticos removibles (CDs, DVDs, discos duros externos, memorias USB) que contengan datos personales, cuando su uso haya finalizado.

5.7.2 Uso de servicios ofimáticos

- Los colaboradores deben solicitar la configuración de las impresoras a Centro de Servicios o su equivalente.

- Siempre que para imprimir sea obligatorio el uso de la contraseña, los colaboradores deberán solicitarla al Centro de Servicios o su equivalente.

- Es responsabilidad de cada colaborador, el destruir inmediatamente los documentos con información interna y confidencial impresos que ya no sirven, usando algún mecanismo de eliminación para evitar manipulación, lectura de la información y reutilización.

- La generación de copias o la reproducción de documentación física contenida en un banco de datos personales únicamente podrán ser realizadas de ser ello necesario, contando con la autorización del responsable del área, en equipos (impresoras, fotocopiadoras, scanner u otros equipos de reproducción) de la UN, y llevándose un registro de las copias y personas autorizadas a tal efecto.

- Se deberán retirar los documentos originales y las copias del equipo (impresora, fotocopiadora, scanner u otro equipo de reproducción) inmediatamente después de finalizada su copia o reproducción.

- Las configuraciones de sistemas de la UN como corporativos en equipos de escritorio, laptops y/o equipos móviles, entregados por la UN o personales, deben ser realizadas exclusivamente por el área de Soporte TI o su equivalente.

5.7.3 Uso de servicios de red

- Los colaboradores no deben usar los servicios de red para acciones no relacionadas a sus funciones.

- Los requerimientos de Home Office permanente deben contar con la aprobación de la Vicepresidencia, Dirección o Gerencia respectiva y ser solicitados a Centro de Servicios o su equivalente.

- No está permitido el uso de dispositivos que brinden acceso a internet a menos que hayan sido otorgados por el área de Sistemas o su equivalente.

- La UN se reserva el derecho de monitorear a través de herramientas de seguridad tecnológica y/o similares, desde su red privada y con respeto al derecho a la intimidad de las personas, el uso de Internet y restringir el acceso a páginas, herramientas, sistemas y/o aplicaciones que vayan en contra de la ética, la moral, las leyes vigentes o las políticas establecidas por Gestión de Desarrollo Humano o su equivalente.

- Los colaboradores son responsables de la información que existe en sus equipos asignados por la UN. No está permitido compartir libremente sus carpetas, siempre deben mantener los niveles de permisos apropiados para las personas o grupos que tendrán acceso (lectura, escritura o modificación). Si el usuario tiene dudas de cómo compartir sus recursos se recomienda contactar a Centro de Servicios o su equivalente.

5.7.4 Uso de correo electrónico

- Los colaboradores solo deberán usar el correo electrónico para las comunicaciones y funciones designadas a su puesto de trabajo.

- Los colaboradores son responsables de todas las actividades que se realicen por medio de sus cuentas de correo electrónico. Los colaboradores no deben utilizar el correo electrónico para fines personales, ni como medio de almacenamiento de información de tipo personal.

- Los colaboradores no deben utilizar el correo para envío de cadenas, spam, archivos de música, videos o archivos ejecutables.

- Los colaboradores no deben abrir correos de dudosa procedencia, de presentarse este caso deberán reportarlo inmediatamente a Seguridad de la Información o su equivalente adjuntando el correo como archivo para la revisión correspondiente.

- Una vez terminada la relación laboral con el colaborador, el jefe y/o inmediato superior podría solicitar el acceso al correo electrónico del usuario, si y solo si, la justificación sea estrictamente requerida para satisfacer la necesidad laboral afectada por la ausencia del colaborador. Asimismo, esta actividad deberá ser revisada y aprobada por la Gerencia de la UN y Seguridad de la UN; asegurando su adecuada documentación y uso de mecanismos de trazabilidad que eviten cualquier alteración o fuga de información no autorizada.

5.7.5 Pantalla y escritorio limpio

- El colaborador deberá bloquear su computadora cuando se aleje de su sitio de trabajo.

- Al momento de retirarse, los colaboradores deberán dejar sus gavetas cerradas. No deberá mantener, en ninguna circunstancia, información confidencial, tales como nombres de cuentas o contraseñas.

5.8. Protección de datos personales

- Lo señalado en la presente sección es sin perjuicio de que a los datos personales también les son de aplicación las demás disposiciones del presente documento, salvo en los casos en que expresamente se indique algo distinto.

- La UN respeta los principios de legalidad, consentimiento, finalidad, proporcionalidad, calidad, disposición de recurso, nivel de protección adecuado, conforme a las disposiciones previstas en la Ley N°29733 – "Ley de protección de datos personales", su reglamento, modificatorias y demás normas conexas.

- El tratamiento de los datos personales, incluida su entrega o transferencia a cualquier tercera persona, se debe realizar solo con previo consentimiento informado, libre, expreso e inequívoco del titular de los datos personales, o salvo que la ley lo autorice.

- No se deben utilizar los datos personales para finalidades distintas a las que motivaron su recopilación.

- Se deberán suprimir los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual hubiesen sido recopilados, hubiese vencido el plazo para su tratamiento, el titular de los datos personales revoque su consentimiento ante la UN, o se produzca algún otro supuesto de cese de tratamiento.

- Todo contrato con proveedores que involucre la recopilación, almacenamiento, tratamiento o entrega de datos personales, debe tener una cláusula de protección de datos personales, confidencialidad y eliminado seguro y total de la data al finalizar el servicio.

- Los procesos internos de la UN involucrados en el tratamiento de datos personales deben ser adecuados y cumplir los requisitos y normas establecidas en la Ley N°29733 – "Ley de protección de datos personales", incluido el cumplimiento de obligaciones formales tales como la inscripción en el Registro Nacional de Protección de Datos Personales de los bancos de datos personales y de ser el caso de las comunicaciones de flujo transfronterizo.

- Las UNs deberán definir formalmente los representantes de cada base de datos específica.

- Las UNs deberán tener implementados canales de atención que se encarguen de tramitar y dar respuesta conforme a ley de las solicitudes que presenten los titulares de datos personales a efectos de ejercer sus derechos de acceso, información, rectificación, oposición, supresión, entre otros.

5.9. Mejora Continua de la Seguridad de la Información

- Las Unidades de Negocio (UN) y Corporativa deben revisar periódicamente y mejorar continuamente sus controles, procesos y sistemas de seguridad de la información, a fin de responder a la evolución de los riesgos cibernéticos, cambios tecnológicos, vulnerabilidades y necesidades del negocio.

- Las áreas de Seguridad de Información, TI, Sistemas o equivalentes deben monitorear la efectividad de las medidas de seguridad de la información mediante evaluaciones internas/externas, auditorías, análisis de incidentes, gestión de vulnerabilidades y pruebas periódicas, asegurando la existencia y ejecución de acciones correctivas y preventivas cuando sea necesario.

- Las lecciones aprendidas derivadas de incidentes de seguridad, auditorías, evaluaciones de riesgos y pruebas de continuidad del negocio deben incorporarse en la mejora continua del marco de gestión de seguridad de la información.

5.10. Monitoreo y Auditoría del Cumplimiento

- Las Unidades de Negocio (UN) y Corporativa deberán realizar evaluaciones y auditorías periódicas para verificar el cumplimiento de la presente Política de Seguridad de la Información y la efectividad de los controles implementados.

- Los hallazgos identificados deberán contar con planes de acción, responsables y seguimiento para asegurar la remediación oportuna y la mejora continua del marco de seguridad de la información.

6. NORMATIVA / DOCUMENTOS RELACIONADOS

- Ley N°29733 – “Ley de protección de datos personales”.
- IRC-TI-PT008 Política Corporativa de Uso Aceptable de Activos.
- IRC-TI-PT007 Política Corporativa de Gestión de Accesos.
- IRC-TI-PT005 Política de seguridad para proveedores.

7. ANEXOS

No aplica