Gestión de seguridad de la información en una bolsa de empleo nacional: diagnóstico, análisis de riesgos y diseño de políticas de seguridad

Corporación Universitaria Remington.
Faculta de Ingeniería
Ingeniería de Sistemas

Juan Sebastian Mancilla Gómez
Jorge Leonardo Ramírez Restrepo
Seminario
2026

Tabla de Contenidos

Resumen

El presente informe desarrolla un análisis integral de seguridad de la información aplicado a una organización dedicada a la intermediación laboral con operaciones a nivel nacional en Colombia. La empresa cuenta con más de 200 empleados distribuidos en oficinas regionales, atiende a más de 1.000 candidatos registrados y a más de 500 empresas clientes a través de un portal web cuya infraestructura opera sobre servicios de computación en la nube.

El análisis parte de la identificación y clasificación de los activos de información de la organización, entre los que se destacan la base de datos de candidatos, la información comercial de empresas clientes, el portal web corporativo y los canales de comunicación institucional. Sobre estos activos se identificaron amenazas activas como ataques de phishing, intentos de acceso no autorizado a la plataforma y uso inadecuado de información por parte de empleados, las cuales encuentran condiciones favorables para materializarse debido a vulnerabilidades estructurales como la ausencia de políticas formales de seguridad, la inexistencia de un área de TI constituida formalmente y la falta de controles de acceso basados en roles.

A partir de una matriz de valoración cualitativa de riesgos basada en probabilidad e impacto, se identificaron tres riesgos críticos: el robo de credenciales mediante phishing, el acceso no autorizado a la base de datos de candidatos y el incumplimiento de la Ley 1581 de 2012, normativa colombiana de protección de datos personales de obligatorio cumplimiento para la organización dado el volumen y naturaleza de la información que gestiona.

En respuesta a los hallazgos del análisis, el informe propone un conjunto de políticas de seguridad prioritarias que incluyen control de acceso, uso aceptable de recursos tecnológicos, protección de datos personales, gestión de incidentes y copias de seguridad. Complementariamente, se diseña un esquema de gestión de incidentes y continuidad del negocio, y se formula un programa de cultura organizacional en seguridad orientado a fortalecer el factor humano como línea de defensa esencial.

El informe concluye que la organización enfrenta un nivel de exposición significativo que requiere acciones inmediatas, y formula recomendaciones priorizadas alineadas con los estándares internacionales ISO 27001 y NIST Cybersecurity Framework, orientadas a elevar progresivamente el nivel de madurez en seguridad de la información de la organización.

Palabras clave

Seguridad de la información, gestión de riesgos, activos de información, vulnerabilidades organizacionales, políticas de seguridad.

Marco conceptual y contextual

Para comprender el análisis desarrollado en el presente informe, es necesario establecer los fundamentos teóricos sobre los cuales se sustenta el estudio de la seguridad de la información en el contexto organizacional. Los conceptos presentados a continuación no solo constituyen la base académica del seminario, sino que guardan una relación directa con la realidad operativa de la organización analizada: una bolsa de empleo de alcance nacional que gestiona datos sensibles de candidatos y empresas clientes a través de canales digitales. Comprender estos conceptos permite identificar con mayor precisión las brechas existentes y las acciones necesarias para fortalecer la protección de la información institucional.

La seguridad de la información se define como el conjunto de medidas, procesos y controles orientados a proteger la información de una organización, garantizando tres propiedades fundamentales conocidas como la triada CIA: confidencialidad, que asegura que la información solo sea accesible para quienes están autorizados; integridad, que garantiza que la información no sea alterada de forma no autorizada; y disponibilidad, que asegura que la información esté accesible cuando sea requerida por los usuarios legítimos (Whitman y Mattord, 2021)d.

En el contexto de la organización analizada, estas tres propiedades son críticas. La confidencialidad es esencial dado que la empresa almacena datos personales de más de 1.000 candidatos y 500 empresas clientes. La integridad es determinante para garantizar que las hojas de vida y los datos de postulación no sean modificados indebidamente. Y la disponibilidad es clave para que el portal web y los servicios digitales operen de forma continua. Por su parte, la ciberseguridad representa una dimensión específica de la seguridad de la información, enfocada en la protección de los sistemas, redes e infraestructuras digitales frente a ataques, accesos no autorizados y otros incidentes de origen cibernético, dimensión especialmente relevante para una organización cuya operación depende en gran medida de servicios en la nube y canales digitales.

Un activo de información es todo elemento que tiene valor para la organización y que, por tanto, requiere ser identificado, clasificado y protegido. Los activos de información no se limitan únicamente a los datos almacenados en sistemas digitales, sino

que abarcan también los procesos, las personas, la infraestructura tecnológica y los canales de comunicación que los soportan. Su identificación es el punto de partida de cualquier análisis de seguridad, dado que no es posible proteger aquello que no se ha reconocido como valioso.

En el caso de la bolsa de empleo analizada, es posible identificar diversos activos de información de alta criticidad. En primer lugar, la base de datos de candidatos, que contiene hojas de vida, documentos de identidad y datos de contacto de más de 1.000 personas registradas. En segundo lugar, la información de las empresas clientes, que incluye datos comerciales, acuerdos de servicio y requerimientos de talento humano de más de 500 organizaciones. En tercer lugar, el portal web corporativo, que actúa como infraestructura central de operación y a través del cual fluye la totalidad de las interacciones digitales. Finalmente, el correo corporativo y los canales de comunicación interna constituyen también activos relevantes, especialmente considerando que parte de la gestión operativa se realiza a través de aplicaciones de mensajería no corporativas. La correcta clasificación de estos activos según su nivel de criticidad y sensibilidad es un requisito fundamental tanto para la norma ISO 27001 como para el cumplimiento de la Ley 1581 de 2012.

Para comprender cómo puede verse comprometida la seguridad de la información en una organización, es necesario distinguir tres conceptos estrechamente relacionados, pero conceptualmente diferentes: amenaza, vulnerabilidad y riesgo. Una amenaza se define como cualquier evento, agente o circunstancia con el potencial de causar daño a los activos de información de una organización (Whitman y Mattord, 2021). Las amenazas pueden tener origen externo, como ataques cibernéticos, phishing o accesos no autorizados, o interno, como el uso inadecuado de la información por parte de empleados. Una vulnerabilidad, por su parte, es una debilidad o carencia presente en los sistemas, procesos o controles de una organización que puede ser explotada por una amenaza para causar un daño. No toda vulnerabilidad representa un problema por sí sola, pero su existencia aumenta significativamente la probabilidad de que una amenaza se materialice.

La relación entre estos dos conceptos da origen al riesgo, entendido como la probabilidad de que una amenaza explote una vulnerabilidad determinada y el impacto que dicho evento tendría sobre la organización. La gestión del riesgo no busca eliminarlo por completo, sino reducirlo a niveles aceptables mediante la implementación de controles adecuados. En el caso de la organización analizada, esta relación es concreta y verificable: la ausencia de políticas formales de seguridad y la falta de un área de TI estructurada constituyen vulnerabilidades que han permitido la materialización de amenazas reales, como los intentos de acceso no autorizado a la plataforma, los ataques de phishing dirigidos al personal y el uso inadecuado de información por parte de empleados. Este escenario configura un perfil de riesgo elevado, especialmente

considerando el volumen y la sensibilidad de los datos que la organización gestiona a diario.

Un control de seguridad es cualquier medida, mecanismo o procedimiento implementado con el propósito de reducir la probabilidad de que una amenaza se materialice, limitar su impacto en caso de que ocurra, o facilitar la recuperación de la organización tras un incidente. Los controles de seguridad se clasifican según su naturaleza en tres categorías: técnicos, administrativos y físicos. Los controles técnicos incluyen medidas como el cifrado de datos, la autenticación de usuarios, los sistemas de detección de intrusos y las copias de seguridad automatizadas. Los controles administrativos comprenden políticas, procedimientos, programas de capacitación y planes de respuesta ante incidentes. Los controles físicos, por su parte, abarcan mecanismos de acceso a instalaciones, custodia de equipos y protección de la infraestructura tecnológica.

Adicionalmente, los controles se clasifican según su función en preventivos, defectivos y correctivos. Los controles preventivos buscan evitar que un incidente ocurra, como las políticas de contraseñas seguras o la restricción de acceso por roles. Los controles defectivos permiten identificar un incidente en curso o ya ocurrido, como los registros de auditoría o las alertas de acceso inusual. Los controles correctivos tienen como objetivo minimizar el daño y restablecer la operación normal tras un incidente, como los planes de recuperación ante desastres o los procedimientos de respuesta a brechas de seguridad. En el contexto de la bolsa de empleo analizada, la ausencia de controles formales en las tres categorías representa una de las principales brechas identificadas, dado que la organización no cuenta con mecanismos documentados que le permitan prevenir, detectar ni responder adecuadamente a los incidentes de seguridad que ya ha experimentado.

La gestión de la seguridad de la información se apoya en estándares internacionales y marcos regulatorios que orientan a las organizaciones sobre cómo estructurar y mejorar sus prácticas de protección. Para el caso analizado, tres referentes son especialmente relevantes.

La norma ISO 27001 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la gestión del riesgo y el ciclo de mejora continua PHVA (International Organization for Standardization, 2022). Su relevancia para la organización es directa: la empresa carece precisamente de los elementos que esta norma exige, como políticas formales, controles documentados y una estructura de gestión de seguridad definida.

El NIST Cybersecurity Framework propone cinco funciones para gestionar la ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar (National Institute of Standards and Technology, 2018). Aplicado al caso de estudio, la organización presenta deficiencias desde la primera función, dado que no ha realizado un inventario formal de activos ni una evaluación estructurada de riesgos, lo que compromete todas las etapas posteriores.

La Ley 1581 de 2012 establece las obligaciones de obligatorio cumplimiento en Colombia para el tratamiento de datos personales, bajo principios como finalidad, necesidad y seguridad. Para una bolsa de empleo que recopila y procesa datos de miles de candidatos, esta ley no es opcional. La ausencia de políticas formales identificada en la organización representa un incumplimiento activo de sus disposiciones, con riesgo de sanciones por parte de la Superintendencia de Industria y Comercio.

Los tres marcos se complementan: la ISO 27001 provee la estructura de gestión, el NIST CSF ofrece un modelo para evaluar la madurez y la Ley 1581 establece las obligaciones legales mínimas sobre las cuales se fundamenta el análisis desarrollado en este informe.

La organización objeto del presente análisis es una bolsa de empleo de alcance nacional con operaciones en Colombia. Su actividad económica principal consiste en la intermediación laboral, actuando como puente entre personas en búsqueda de empleo y empresas que requieren talento humano. Para cumplir este propósito, la organización ofrece servicios de publicación de vacantes, gestión de hojas de vida y conexión entre candidatos y empleadores.

La empresa cuenta con más de 200 empleados distribuidos en oficinas a lo largo del territorio nacional, lo que le permite brindar atención presencial a sus usuarios en diferentes regiones del país. Adicionalmente, opera a través de un portal web que centraliza sus servicios digitales, mediante el cual más de 1.000 candidatos registrados y más de 500 empresas clientes acceden a las funcionalidades de la plataforma. Esta combinación de canales —digital y presencial— define el modelo operativo de la organización y determina en gran medida el flujo y volumen de información que gestiona cotidianamente.

La organización presenta una estructura distribuida por regiones, con oficinas de atención al cliente ubicadas en diferentes ciudades del país, cada uno operando de manera semiautónoma bajo los lineamientos de una dirección central. Esta configuración le permite mantener presencia territorial y atender de forma directa tanto a candidatos como a empresas clientes en distintas zonas geográficas de Colombia.

En cuanto a su composición interna, la empresa cuenta con áreas funcionales orientadas a la operación comercial, la atención al usuario y la gestión administrativa, distribuidas entre su planta de más de 200 empleados. Si bien dispone de personal con conocimientos en tecnología de la información que da soporte a los sistemas y al portal web, no existe un área formal de TI constituida como unidad independiente dentro de la estructura organizacional. Esto implica que las decisiones relacionadas con la gestión tecnológica y los sistemas de información recaen de manera difusa entre la dirección general y el personal técnico disponible, sin una jerarquía claramente definida para estos asuntos.

Los procesos centrales de la organización giran en torno a la intermediación laboral y se desarrollan a través de dos ejes principales: la gestión de candidatos y la gestión de empresas clientes. En el primer caso, el proceso comprende el registro de personas en búsqueda de empleo, la recopilación de información personal y documentos como hojas de vida, datos de identidad y datos de contacto, así como la administración de postulaciones a vacantes disponibles. En el segundo eje, la organización gestiona el registro y seguimiento de más de 500 empresas clientes, incluyendo información comercial, publicación de vacantes y coordinación de procesos de selección.

Ambos flujos de información convergen en el portal web corporativo, que actúa como plataforma central de operación y a través del cual se realizan la mayoría de las interacciones entre la organización, los candidatos y las empresas. Los datos generados por estos procesos se almacenan en servicios de computación en la nube, lo que permite disponibilidad y acceso remoto desde las distintas oficinas regionales del país. Para la comunicación interna y externa, la organización emplea correo corporativo como canal formal; sin embargo, se ha identificado el uso de aplicaciones de mensajería instantánea y redes sociales como canales informales para la gestión operativa del día a día, práctica que introduce variables adicionales en el control y trazabilidad de la información institucional.

La organización desarrolla su actividad en un entorno altamente regulado en materia de protección de datos personales. En Colombia, el marco normativo principal que rige el tratamiento de información personal es la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales (Congreso de la República de Colombia, 2012), reglamentada por el Decreto 1377 de 2013. Esta normativa establece los principios, derechos y obligaciones que deben observar las organizaciones que recopilan, almacenan, usan o transfieren datos personales, lo cual aplica directamente a una bolsa de empleo dado el volumen y la naturaleza de la información que maneja sobre candidatos y empresas.

Adicionalmente, la Superintendencia de Industria y Comercio (SIC) actúa como autoridad de control y vigilancia en esta materia, con facultades sancionatorias frente a organizaciones que incumplan las disposiciones sobre habeas data y tratamiento de datos. En este sentido, la organización está obligada a contar con políticas de privacidad, mecanismos de autorización para el tratamiento de datos y procedimientos para atender solicitudes de los titulares de la información.

Desde el punto de vista del entorno competitivo y tecnológico, el sector de intermediación laboral en Colombia ha experimentado una marcada transformación digital, acelerada especialmente a partir de 2020. Esta evolución ha incrementado significativamente el volumen de datos gestionados en línea y ha ampliado la superficie de exposición a riesgos cibernéticos, exigiendo a las organizaciones del sector una mayor madurez en sus prácticas de seguridad de la información.

La organización presenta una situación de vulnerabilidad notable en materia de seguridad de la información. A la fecha, no cuenta con políticas formales documentadas que regulen el tratamiento, acceso, almacenamiento o disposición de la información institucional, lo que significa que las decisiones relacionadas con la protección de datos se toman de manera reactiva y sin criterios estandarizados. Esta ausencia de un marco normativo interno es especialmente crítica considerando que la empresa gestiona datos personales sensibles de más de 1.000 candidatos y de 500 empresas clientes, información que está sujeta a las obligaciones establecidas por la Ley 1581 de 2012.

A nivel operativo, se han identificado situaciones concretas que evidencian las necesidades de la organización en este ámbito. Se han registrado intentos de acceso no autorizado a la plataforma web, así como ataques de phishing dirigidos a empleados a través del correo corporativo, lo que expone la falta de controles técnicos y de concienciación del personal frente a amenazas externas. Adicionalmente, se ha detectado uso inadecuado de información por parte de empleados, situación que refleja la ausencia de controles de acceso basados en roles y de procedimientos claros sobre el manejo interno de los datos. A esto se suma el uso de canales informales como aplicaciones de mensajería instantánea para la gestión operativa, lo cual dificulta la trazabilidad y el control de la información que circula dentro de la organización.

En conjunto, este panorama justifica plenamente el desarrollo del presente informe. La combinación de un alto volumen de datos sensibles, una infraestructura tecnológica en la nube sin políticas de seguridad que la respalden, incidentes ya materializados y la ausencia de un área formal de TI, configura un escenario de riesgo que demanda un análisis estructurado orientado a identificar brechas y proponer controles alineados con las buenas prácticas de seguridad de la información.

1. Identificación y Clasificación de Activos de Información

1.1. Inventario de activos.

La identificación de los activos de información es el punto de partida de cualquier proceso de gestión de seguridad, ya que no es posible proteger aquello que no ha sido reconocido y catalogado. En el caso de la bolsa de empleo analizada, los activos de información se distribuyen en cuatro categorías principales: datos, sistemas, personas e infraestructura.

1.2. Activos de datos.

Los activos de datos constituyen el núcleo más sensible de la organización, dado que su actividad gira en torno a la recopilación, almacenamiento y procesamiento de información personal. Entre los principales activos de datos se identifican los siguientes:

- Hojas de vida y datos personales de candidatos: nombres, números de identificación, datos de contacto, experiencia laboral, nivel educativo y documentos adjuntos de más de 1.000 usuarios registrados. Esta información es considerada dato personal bajo la Ley 1581 de 2012 y requiere medidas de protección específicas.
- Información de empresas clientes: razón social, datos de contacto, información comercial, descripción de vacantes y acuerdos de servicio de más de 500 organizaciones registradas en la plataforma.
- Registros de postulaciones y procesos de selección: historial de aplicaciones, estados de los procesos y comunicaciones entre candidatos y empresas.
- Datos de acceso y autenticación: credenciales de usuarios, registros de inicio de sesión y tokens de acceso al portal web.
- Comunicaciones internas: correos corporativos, mensajes intercambiados a través de aplicaciones de mensajería y documentos compartidos entre empleados.

1.3. Activos de sistemas e infraestructura tecnológica

- Portal web corporativo: plataforma principal de operación a través de la cual se realizan los procesos de registro, postulación y gestión de vacantes. Constituye el activo tecnológico de mayor criticidad dado que centraliza toda la operación digital de la empresa.

- Infraestructura en la nube: servicios de almacenamiento y procesamiento contratados con proveedores de nube pública, donde residen las bases de datos y los sistemas de la organización.
- Correo corporativo: canal formal de comunicación interna y externa, utilizado tanto para la gestión operativa como para el envío de notificaciones a candidatos y empresas.
- Equipos de cómputo y dispositivos: computadores, teléfonos corporativos y demás dispositivos utilizados por los más de 200 empleados distribuidos en las oficinas regionales.

1.4. Activos humanos y de proceso

El personal de la organización constituye también un activo de información crítico, especialmente aquellos empleados con acceso privilegiado a bases de datos, sistemas administrativos o información confidencial de clientes. Igualmente, los procesos operativos documentados — o la ausencia de su documentación — representan activos intangibles cuya pérdida o compromiso puede afectar significativamente la continuidad del negocio.

1.5 Clasificación de activos por nivel de criticidad

Activo	Categoría	Nivel de Criticidad	Justificación
Base de datos de candidatos	Datos	Alto	Su compromiso afectaría directamente a más de 1.000 personas, generaría sanciones bajo la Ley 1581 y destruiría la confianza de los usuarios en la plataforma
Información de empresas clientes	Datos	Alto	Su filtración podría romper relaciones comerciales con más de 500 empresas y generar pérdida de contratos y reputación corporativa
Portal web corporativo	Sistema	Alto	Es el canal principal de operación. Su caída detendría completamente el servicio a nivel nacional, afectando todas

			las oficinas regionales simultáneamente
Infraestructura en la nube	Infraestructura	Alto	Soporta la totalidad de los datos y sistemas. Un fallo sin plan de continuidad implicaría la pérdida total de la operación digital de la empresa
Credenciales de acceso	Datos	Alto	Su robo permitiría a un atacante suplantar empleados, acceder a datos sensibles y operar dentro del sistema sin ser detectado
Correo corporativo	Sistemas	Medio	Su afectación interrumpiría las comunicaciones formales, pero la operación presencial en oficinas podría mantenerse temporalmente
Equipo de computo	Infraestructura	Medio	Su pérdida o daño afecta la productividad local de cada oficina, pero no detiene la operación nacional si el portal web permanece disponible
Comunicaciones por mensajería	Datos	Medio	Aunque su uso es informal, contiene información operativa sensible cuya exposición podría derivar en fugas de datos no controladas
Personal con acceso privilegiado	Humano	Alto	Su desvinculación sin revocar accesos o su actuación malintencionada representa uno de los vectores de riesgo interno más difíciles de detectar y controlar

2. Amenazas y Vulnerabilidades

2.1 Definición del panorama de amenazas

Una amenaza representa cualquier evento o agente con capacidad de causar daño a los activos de información de la organización. En el sector de intermediación laboral, donde se manejan volúmenes significativos de datos personales a través de plataformas digitales, el panorama de amenazas es amplio y varía tanto en origen como en impacto. Las amenazas pueden clasificarse en externas, cuando provienen de agentes ajenos a la organización, e internas, cuando se originan dentro de la misma, ya sea por negligencia o por acción deliberada del personal.

2.2 Amenazas externas identificadas

2.2.1 Phishing y ingeniería social

El phishing es una de las amenazas más frecuentes y de mayor impacto en organizaciones que operan principalmente a través de canales digitales. Consiste en el envío de comunicaciones fraudulentas, generalmente por correo electrónico, que suplantan la identidad de entidades legítimas con el objetivo de engañar a los empleados para que revelen credenciales de acceso o información confidencial. La organización analizada ha registrado ataques de este tipo dirigidos a su personal, lo que evidencia que esta amenaza no es hipotética sino activa y recurrente.

2.2.2 Accesos no autorizados a la plataforma

Los intentos de acceso no autorizado al portal web representan una amenaza directa sobre los activos de datos más críticos de la organización. Este tipo de ataque puede materializarse mediante el uso de credenciales robadas, ataques de fuerza bruta sobre contraseñas débiles o la explotación de vulnerabilidades en el código de la plataforma. La organización ha identificado incidentes de este tipo, lo que indica la existencia de debilidades en sus mecanismos de autenticación y control de acceso.

2.2.3 Ataques a la infraestructura en la nube

Al operar sobre servicios de computación en la nube, la organización está expuesta a amenazas específicas de este entorno, como configuraciones incorrectas de permisos, accesos no autorizados a contenedores de almacenamiento o interceptación de

datos en tránsito. La ausencia de políticas formales de seguridad aumenta el riesgo de que estos entornos no estén correctamente configurados ni monitoreados.

2.3 Amenazas internas identificadas

2.3.1 Uso inadecuado de la información por parte de empleados

Se ha identificado que empleados de la organización han hecho uso inadecuado de la información a la que tienen acceso debido a sus funciones. Esta amenaza puede manifestarse como la divulgación no autorizada de datos de candidatos o empresas clientes, la consulta de información fuera del ámbito de las responsabilidades del cargo, o la transferencia de datos a canales no seguros. Este tipo de incidente es especialmente crítico en organizaciones sin políticas de control de acceso basadas en roles.

2.3.2 Uso de canales informales de comunicación

El uso de aplicaciones de mensajería instantánea y redes sociales para la gestión operativa introduce una amenaza interna significativa, ya que estos canales no están bajo el control de la organización, no garantizan la confidencialidad de la información transmitida y no dejan registros auditables. La información institucional que circula por estos medios queda expuesta a terceros y escapa a cualquier mecanismo de monitoreo o trazabilidad.

2.4 Vulnerabilidades identificadas

Las vulnerabilidades son las debilidades presentes en la organización que facilitan que las amenazas descritas anteriormente puedan materializarse. A continuación, se presentan las principales vulnerabilidades identificadas:

Vulnerabilidad	Area afectada	Nivel de exposición
Ausencia de politicas formales de seguridad	Toda la organización	Alto
Inexistencia de un área formal de TI	Gestión tecnológica	Alto
Falta de controles de acceso basado en roles	Sistemas y datos	Alto
Uso de canales informales para gestion operativa	comunicaciones	Medio
Ausencia de programas de concienciacion al personal	Talento humano	Alto

Falta de monitoreo y auditoria de accesos	Infraestructura	Alto
Posibles configuraciones inadecuadas en la nube	Infraestructura	Medio
Ausencia de procedimientos de repuestas a incidentes	Operaciones	Alto

2.5 Relación entre amenazas y vulnerabilidades

La combinación de las amenazas identificadas con las vulnerabilidades existentes no solo genera riesgos técnicos, sino que tiene consecuencias directas sobre la operación nacional y la reputación de la organización.

Un ataque de phishing exitoso que comprometa las credenciales de un empleado con acceso privilegiado podría permitir el ingreso no autorizado a la base de datos de candidatos, resultando en la exposición masiva de datos personales de miles de personas.

Este tipo de incidente, además de generar sanciones legales por parte de la Superintendencia de Industria y Comercio, tendría un impacto reputacional severo: una bolsa de empleo cuya función esencial es la gestión de datos personales que sufre una filtración masiva pierde inmediatamente la confianza de candidatos y empresas clientes, poniendo en riesgo su continuidad en el mercado.

Un acceso no autorizado al portal web que resulte en su indisponibilidad prolongada afectaría simultáneamente a todas las oficinas regionales del país, dado que la operación digital centralizada en esta plataforma no cuenta con procedimientos alternativos formales documentados. En una organización de alcance nacional, una caída del sistema sin plan de continuidad puede traducirse en cientos de procesos de selección interrumpidos, pérdida de contratos con empresas clientes y daño directo a la imagen institucional frente a competidores del sector.

El uso inadecuado de información por parte de empleados, facilitado por la ausencia de controles de acceso basados en roles, representa una amenaza interna cuyo impacto puede ser igual o mayor al de un ataque externo. Un empleado que accede y divulga datos de candidatos o empresas clientes sin autorización puede generar demandas legales, pérdida de clientes estratégicos y cobertura negativa en medios, todo ello en un contexto donde la organización no cuenta con un protocolo de respuesta que le permita actuar con rapidez y contener el daño reputacional.

Finalmente, el uso de canales informales de comunicación como aplicaciones de mensajería personal para gestionar información operativa representa una fuga de datos silenciosa y continua que la organización no puede detectar ni controlar. A diferencia de un ataque externo puntual, esta vulnerabilidad opera de manera permanente y acumulativa, exponiendo progresivamente información sensible de candidatos y empresas a entornos fuera del control institucional.

3. Análisis y Gestión de Riesgos

3.1 Metodología de análisis de riesgos

El análisis de riesgos permite determinar el nivel de exposición de la organización a partir de la relación entre las amenazas identificadas y las vulnerabilidades existentes. Para el presente informe se adopta una metodología cualitativa basada en dos variables: la probabilidad de ocurrencia de cada riesgo y el impacto que tendría su materialización sobre los activos de información y la operación de la organización. La combinación de estas dos variables genera un nivel de riesgo que puede ser clasificado como bajo, medio, alto o crítico, permitiendo priorizar las acciones de tratamiento de manera ordenada y justificada.

3.2 Escala de valoración

Para la evaluación de cada riesgo se utilizan las siguientes escalas:

Probabilidad de ocurrencia:

Nivel	Descripción
1- Baja	El evento raramente ocurre o no se ha registrado antecedentes
2- Media	El evento podría ocurrir en algún momento o ha ocurrido ocasionalmente
3- Alta	El evento ocurre con frecuencia o ya se ha materializado en la organización

Impacto:

Nivel	Descripción
1- Bajo	Afectación mínima, sin consecuencias operativas

2- Medio	Afectación parcial de la operación, posible consecuencias legales o reputacionales
3- Alto	Afectación grave de la operación. Sanciones legales pérdida de confianza de clientes

Nivel de riesgo = Probabilidad × Impacto:

Resultado	Nivel de riesgo
1 - 2	Bajo
3 - 5	Medio
6 - 9	Alto / Critico

3.3 Matriz de riesgos

La valoración de cada riesgo no se realizó de manera arbitraria sino a partir de dos criterios concretos. Para determinar la probabilidad, se consideró la evidencia disponible sobre la situación actual de la organización: los riesgos calificados con probabilidad alta (3) corresponden a amenazas que ya se han materializado en la empresa — como el phishing, los accesos no autorizados y el uso inadecuado de información — o a vulnerabilidades estructurales tan evidentes que hacen casi inevitable su explotación, como el incumplimiento de la Ley 1581 ante la ausencia total de políticas de privacidad.

Los riesgos con probabilidad media (2) corresponden a escenarios que aún no se han confirmado como incidentes pero cuyas condiciones están presentes, como las posibles configuraciones inadecuadas en la nube o la indisponibilidad del portal web.

Para determinar el impacto, se evaluó la consecuencia que tendría la materialización de cada riesgo sobre tres dimensiones: la continuidad operativa de la organización a nivel nacional, la integridad y confidencialidad de los datos de candidatos y empresas clientes, y la exposición legal bajo la Ley 1581 de 2012. Los riesgos calificados con impacto alto (3) son aquellos cuya ocurrencia afectaría simultáneamente más de una de estas dimensiones, como una brecha en la base de datos de candidatos que implicaría tanto la interrupción operativa como sanciones legales y daño reputacional. Los riesgos con impacto medio (2) afectan principalmente la operación interna sin comprometer masivamente datos personales ni generar consecuencias legales inmediatas.

#	Riesgo identificado	Activo afectado	Probabilidad	Impacto	Nivel de riesgo

R1	Robo de credenciales mediante phishing	Credenciales de acceso/portal web	3	3	Critico (9)
R2	Acceso no autorizado a la base de datos de candidatos	Base de datos de candidatos	3	3	Critico (9)
R3	Filtración de datos de empresas clientes	Información de empresas clientes	2	3	Alto (6)
R4	Uso inadecuado de información por empleados	Datos de candidatos y clientes	3	2	Alto (6)
R5	Fuga de información por canales informales	Comunicaciones internas	3	2	Alto (6)
R6	Configuración inadecuada de servicio en la nube	Infraestructura en la nube	2	3	Alto (6)
R7	Indisponibilidad del portal web por ataque	Portal web corporativo	2	3	Alto (6)
R8	Incumplimiento de la ley 1581 de 2012	Toda la organización	3	3	Critico (9)
R9	Perdida de información por ausencia de copias de seguridad	Base de datos / infraestructura	2	3	Alto (6)
R10	Ausencia de repuesta estructurada ante incidentes	Operaciones	3	2	Alto (6)

3.4 Análisis de los riesgos críticos

Los riesgos clasificados como críticos merecen atención prioritaria dado su alto nivel de probabilidad e impacto simultáneo.

R1 — Robo de credenciales mediante phishing: dado que la organización ya ha registrado ataques de phishing dirigidos a su personal y no cuenta con programas de concienciación ni controles técnicos de autenticación robustos como la verificación en dos pasos, la probabilidad de que este riesgo se materialice con éxito es alta. Su impacto es igualmente crítico, ya que el compromiso de credenciales de acceso podría permitir el ingreso no autorizado al portal web y a la base de datos de candidatos.

R2 — Acceso no autorizado a la base de datos de candidatos: la combinación de intentos de acceso no autorizado ya registrados y la ausencia de controles de acceso basados en roles hace de este riesgo uno de los más urgentes. Su materialización implicaría la exposición de datos personales de más de 1.000 candidatos, con consecuencias legales directas bajo la Ley 1581 de 2012.

R8 — Incumplimiento de la Ley 1581 de 2012: la ausencia de políticas formales de seguridad, la falta de mecanismos documentados de autorización para el tratamiento de datos y la inexistencia de procedimientos para atender solicitudes de los titulares de la información configuran un incumplimiento activo de las obligaciones establecidas por esta normativa, lo que expone a la organización a sanciones por parte de la Superintendencia de Industria y Comercio.

3.5 Tratamiento de riesgos

Una vez identificados y valorados los riesgos, la organización debe definir una estrategia de tratamiento para cada uno. Las opciones disponibles son cuatro: mitigar el riesgo mediante la implementación de controles, transferirlo a un tercero como una aseguradora o proveedor especializado, aceptarlo cuando su nivel es bajo y el costo de mitigación supera el beneficio, o evitarlo eliminando la actividad que lo genera.

#	Riesgo	Estrategia	Acción prioritaria
R1	Robo de credenciales por phishing	Mitigar	Capacitación al personal y autenticación de dos factores

R2	Acceso no autorizado a base de datos	Mitigar	Control de acceso por roles y monitoreo de accesos
R3	Filtración de datos de clientes	Mitigar	Cifrado de datos y acuerdos de confidencialidad
R4	Uso inadecuado de información	Mitigar	Políticas de uso aceptable y control de acceso
R5	Fuga por canales informales	Evitar / Mitigar	Prohibición formal y canales corporativos seguros
R6	Configuración inadecuada en la nube	Mitigar	Auditoría de configuración y gestión de permisos
R7	Indisponibilidad del portal web	Trasferir / Mitigar	Acuerdo de nivel de servicio con proveedor en la nube
R8	Incumplimiento Ley 1581	Mitigar	Implementación de política de privacidad y tratamiento de datos
R9	Pérdida de información	Mitigar	Plan de copias de seguridad automatizadas
R10	**Ausencia de respuesta a incidentes**	Mitigar	Diseño de plan de respuesta ante incidentes

4. Diseño de Políticas de Seguridad

4.1 Justificación y enfoque

La ausencia de políticas formales de seguridad constituye la vulnerabilidad más transversal identificada en el análisis, ya que su inexistencia afecta directamente todos los controles y procesos de la organización. Un aspecto particular del contexto de la empresa es que actualmente no cuenta con un área formal de TI, lo que significa que la implementación y supervisión de estas políticas deberá apoyarse en el personal técnico

disponible bajo una estructura de responsabilidades claramente asignada y respaldada por la dirección general. En respuesta a los riesgos identificados, se presentan a continuación las políticas prioritarias que la organización debe implementar.

4.2 Política de control de acceso

Objetivo: garantizar que únicamente el personal autorizado acceda a los sistemas y datos de la organización según su rol y responsabilidades.

Lineamientos principales:

- Todo empleado deberá contar con credenciales de acceso individuales e intransferibles para los sistemas corporativos. Queda estrictamente prohibido compartir usuarios o contraseñas entre compañeros.
- El acceso a la información deberá otorgarse bajo el principio de mínimo privilegio, es decir, cada empleado tendrá acceso únicamente a la información estrictamente necesaria para el desempeño de sus funciones.
- Se implementará autenticación de doble factor para el acceso al portal web corporativo y a los servicios en la nube.
- Las credenciales de acceso deberán renovarse cada noventa días y cumplir con requisitos mínimos de complejidad: mínimo ocho caracteres, combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- El área de TI deberá revisar y actualizar los permisos de acceso cada vez que un empleado cambie de cargo o se desvincule de la organización.

Implementación operativa: dado que la organización no cuenta con un área formal de TI, se deberá designar a uno de los técnicos disponibles como administrador de accesos, con autoridad y tiempo dedicado específicamente a esta función. Este administrador será responsable de crear, modificar y revocar permisos en el portal web y los servicios en la nube cada vez que se vincule o desvincule un empleado, o cuando cambie de cargo. La definición de roles deberá realizarse en conjunto con cada líder de área, quien conoce qué información necesita su equipo para operar. Como punto de partida práctico, se sugieren al menos tres perfiles de acceso: administrador para el personal de TI, operativo para empleados que gestionan candidatos y vacantes, y consulta para personal de apoyo administrativo. El cumplimiento de esta política deberá revisarse trimestralmente mediante un reporte de accesos activos que el administrador presentará a la dirección general.

4.3 Política de uso aceptable de recursos tecnológicos

Objetivo: establecer los usos permitidos y prohibidos de los recursos tecnológicos de la organización, incluyendo equipos, sistemas, correo corporativo e internet.

Lineamientos principales:

- Los equipos de cómputo, el correo corporativo y los sistemas de la organización son de uso exclusivamente laboral. Su uso para actividades personales, comerciales ajenas a la empresa o de entretenimiento no está permitido durante la jornada laboral.
- Queda prohibido el uso de aplicaciones de mensajería instantánea de carácter personal, como WhatsApp u otras redes sociales, para el intercambio de información institucional, datos de candidatos o información de empresas clientes. Toda comunicación operativa deberá realizarse a través de los canales corporativos oficiales.
- No está permitida la instalación de software no autorizado en los equipos corporativos.
- El personal no deberá acceder a los sistemas de la organización desde redes públicas o no seguras sin el uso de una red privada virtual (VPN).

Implementación operativa: la transición desde el uso actual de canales informales hacia canales corporativos exclusivos debe gestionarse de forma gradual. Como primer paso, la dirección deberá comunicar formalmente la prohibición mediante un mensaje oficial dirigido a todos los empleados, explicando el motivo de la medida y el canal alternativo habilitado. Para que la política sea efectiva, la organización deberá garantizar que el correo corporativo funcione correctamente en dispositivos móviles, de modo que los empleados en oficinas regionales puedan comunicarse con la misma agilidad que ofrece la mensajería informal. El cumplimiento podrá supervisarse a través de revisiones periódicas del correo corporativo y mediante reportes de incidentes relacionados con el uso de canales no autorizados.

4.4 Política de protección de datos personales

Objetivo: garantizar el cumplimiento de la Ley 1581 de 2012 y asegurar que el tratamiento de datos personales de candidatos y empresas clientes se realice de manera legal, segura y transparente.

Lineamientos principales:

- La organización deberá contar con un aviso de privacidad visible en el portal web que informe a los titulares sobre la finalidad del tratamiento de sus datos, los derechos que les asisten y los canales para ejercerlos.
- Todo candidato o empresa que se registre en la plataforma deberá otorgar su autorización expresa para el tratamiento de sus datos personales, de conformidad con lo establecido en la Ley 1581 de 2012.
- Los datos personales de candidatos y empresas clientes no podrán ser compartidos con terceros sin la autorización previa y expresa de sus titulares, salvo en los casos expresamente contemplados por la ley.
- La organización deberá designar un responsable del tratamiento de datos personales, encargado de atender las solicitudes de acceso, corrección, actualización o supresión de información por parte de los titulares.
- Los datos personales deberán almacenarse con medidas de cifrado adecuadas y solo durante el tiempo necesario para cumplir la finalidad para la que fueron recopilados.

Implementación operativa: el responsable del tratamiento de datos no requiere ser necesariamente un abogado o especialista externo. En una organización sin área de TI formal, esta función puede asignarse a un empleado de confianza con perfil administrativo o jurídico, capacitado en los principios de la Ley 1581. Sus responsabilidades concretas incluirán atender las solicitudes de candidatos que deseen consultar, corregir o eliminar sus datos, mantener actualizado el registro de actividades de tratamiento y verificar anualmente que el aviso de privacidad del portal esté vigente y sea coherente con el uso real que se da a los datos.

4.5 Política de gestión de incidentes de seguridad

Objetivo: establecer los procedimientos que deben seguirse cuando se detecte o sospeche un incidente de seguridad de la información, garantizando una respuesta oportuna y estructurada.

Lineamientos principales:

- Todo empleado que detecte o sospeche un incidente de seguridad, como un acceso no autorizado, la pérdida de un dispositivo, un correo de phishing o el uso indebido de información, deberá reportarlo de inmediato al responsable de TI o al superior jerárquico correspondiente.
- La organización deberá mantener un registro formal de todos los incidentes reportados, incluyendo fecha, descripción, activos afectados, acciones tomadas y resultado.

- Ante un incidente que comprometa datos personales de candidatos o empresas clientes, la organización deberá notificar a la Superintendencia de Industria y Comercio en los términos establecidos por la normativa vigente.
- Los incidentes deberán analizarse una vez resueltos con el fin de identificar su causa raíz y definir acciones correctivas que eviten su recurrencia.

Implementación operativa: dado que la organización no tiene un área de seguridad dedicada, el monitoreo de incidentes deberá apoyarse en herramientas accesibles y de bajo costo. Los servicios en la nube que utiliza la empresa — como AWS, Azure o Google Cloud — incluyen por defecto registros de actividad y alertas configurables que permiten detectar accesos inusuales, intentos fallidos de autenticación o modificaciones no autorizadas en los datos. El administrador de accesos designado deberá revisar estos registros con una frecuencia mínima semanal. Para el reporte interno de incidentes, basta con habilitar un canal simple y conocido por todos los empleados, como una dirección de correo corporativo dedicada exclusivamente a este fin, de modo que cualquier persona pueda reportar una situación sospechosa sin necesidad de estructuras complejas.

4.6 Política de copias de seguridad

Objetivo: garantizar la disponibilidad e integridad de la información crítica de la organización mediante la realización periódica de copias de seguridad.

Lineamientos principales:

- Se realizarán copias de seguridad automáticas de las bases de datos del portal web y de los sistemas corporativos con una frecuencia mínima diaria.
- Las copias de seguridad deberán almacenarse en una ubicación diferente a la de los datos originales, preferiblemente en un servicio de almacenamiento en la nube independiente del entorno principal de producción.
- La integridad y disponibilidad de las copias de seguridad deberá verificarse mediante pruebas de restauración realizadas al menos una vez cada trimestre.
- El acceso a las copias de seguridad deberá estar restringido al personal autorizado y registrado en la política de control de acceso.

Implementación operativa: los proveedores de nube que utiliza actualmente la organización ofrecen funciones nativas de copia de seguridad automatizada que pueden activarse sin necesidad de desarrollos adicionales ni infraestructura propia. El administrador de TI deberá configurar estas copias para que se ejecuten diariamente en horario de baja actividad y verificar mensualmente que el proceso se haya completado sin errores. La prueba de restauración trimestral no requiere afectar el entorno productivo —

puede realizarse en un entorno de prueba separado — y su resultado deberá quedar documentado como evidencia del funcionamiento del respaldo.

4.7 Responsabilidades y cumplimiento

La implementación y cumplimiento de las políticas descritas es responsabilidad de todos los niveles de la organización. La dirección general es responsable de aprobar, comunicar y garantizar los recursos necesarios para su aplicación. El personal de TI es responsable de implementar los controles técnicos que respaldan cada política. Y todos los empleados, independientemente de su cargo o ubicación, están obligados a conocer y cumplir los lineamientos establecidos. El incumplimiento de estas políticas podrá derivar en medidas disciplinarias internas y, en caso de afectar datos personales, en consecuencias legales bajo la normativa colombiana vigente.

5. Gestión de Incidentes, Respuesta y Continuidad

5.1 Importancia de la gestión de incidentes

Ninguna organización está completamente exenta de sufrir incidentes de seguridad de la información, independientemente del nivel de madurez de sus controles. Lo que diferencia a una organización preparada de una que no lo está es su capacidad de detectar, responder y recuperarse de dichos incidentes de manera estructurada, minimizando el impacto sobre sus operaciones, sus activos y su reputación. Para la organización analizada, cuya situación actual evidencia incidentes ya materializados y la ausencia de procedimientos formales de respuesta, el diseño de un esquema de gestión de incidentes y continuidad representa una necesidad inmediata.

5.2 Clasificación de incidentes de seguridad

Para gestionar los incidentes de manera ordenada, es necesario clasificarlos según su naturaleza y nivel de impacto. La siguiente clasificación permite priorizar la respuesta y asignar los recursos adecuados en función de la gravedad de cada evento.

Nivel	Clasificación	Descripción	Ejemplo aplicado
1	Bajo	Evento menor sin impacto operativo significativo	Correo de phishing recibido, pero no ejecutado
2	Medio	Afectación parcial de sistemas o datos sin compromiso masivo	Acceso no autorizado a una cuenta de usuario individual

3	Alto	Compromiso de sistemas críticos o datos sensibles de múltiples usuarios	Brecha en la base de datos de candidatos
4	Critico	Afectación grave de la operación con consecuencias legales o reputacionales severas	Filtración masiva de datos personales o caída total del portal web

5.3 Procedimiento de respuesta ante incidentes

El procedimiento de respuesta ante incidentes establece las fases y acciones que deben ejecutarse desde el momento en que se detecta un evento de seguridad hasta su resolución definitiva. Este procedimiento está alineado con las recomendaciones del NIST Cybersecurity Framework en sus funciones de Detectar, Responder y Recuperar.

Fase 1 — Detección e identificación

La detección puede originarse a través de diferentes mecanismos: alertas automáticas del sistema, reportes del personal, monitoreo de accesos o notificaciones de usuarios externos. Una vez detectado un posible incidente, el empleado que lo identifica deberá reportarlo de inmediato al responsable de TI mediante el canal oficial establecido para tal fin. En esta fase se debe registrar la fecha y hora del evento, los sistemas o activos afectados, la descripción del comportamiento anómalo observado y la identidad de quien reporta.

Fase 2 — Contención

El objetivo de esta fase es limitar el alcance del incidente y evitar que se propague a otros sistemas o activos. Las acciones de contención dependen del tipo de incidente:

- Ante un acceso no autorizado: suspender de inmediato las credenciales comprometidas y bloquear el acceso desde las direcciones IP identificadas como maliciosas.
- Ante un ataque de phishing exitoso: aislar el equipo afectado de la red corporativa y restablecer las credenciales del usuario comprometido.
- Ante una fuga de información: identificar el canal por el cual se produjo la filtración y restringir el acceso a los datos afectados.

Fase 3 — Erradicación

Una vez contenido el incidente, se debe identificar y eliminar la causa raíz que lo originó. Esto puede implicar la eliminación de software malicioso, la corrección de configuraciones incorrectas en los sistemas o la revocación de accesos indebidos. En esta fase es fundamental no restaurar los sistemas afectados hasta confirmar que la amenaza ha sido completamente neutralizada.

Fase 4 — Recuperación

La fase de recuperación tiene como objetivo restablecer la operación normal de los sistemas y servicios afectados de manera segura y controlada. Se deben restaurar los datos desde las copias de seguridad verificadas, confirmar que los sistemas funcionan correctamente antes de reintegrarlos al entorno de producción y notificar a los usuarios y áreas afectadas sobre el restablecimiento del servicio.

Fase 5 — Lecciones aprendidas

Una vez resuelto el incidente, el equipo responsable deberá elaborar un informe post-incidente que incluya la descripción detallada del evento, la línea de tiempo de la respuesta, el impacto real sobre los activos y la operación, las acciones tomadas en cada fase y las recomendaciones para evitar que el incidente se repita. Este informe debe quedar registrado en el historial de incidentes de la organización y ser utilizado como insumo para la mejora continua de los controles de seguridad.

5.4 Roles y responsabilidades en la gestión de incidentes

Para que el procedimiento descrito funcione en la práctica, la organización debe definir claramente quién es responsable de qué en cada fase del proceso.

Rol	Responsabilidad
Todo el personal	Detectar y reportar incidentes sospechosos de inmediato
Responsable de TI	Coordinar la respuesta técnica, contención y erradicación
Dirección general	Tomar decisiones sobre notificación a autoridades y comunicación externa
Responsable de datos personales	Evaluar si el incidente implica notificación a la SIC bajo la Ley 1581
Todas las áreas afectadas	Colaborar en la fase de recuperación y documentación

5.5 Plan de continuidad del negocio

El plan de continuidad del negocio tiene como propósito garantizar que la organización pueda mantener sus operaciones esenciales durante y después de un incidente grave. Para la bolsa de empleo analizada, cuya operación depende críticamente del portal web y los servicios en la nube, una interrupción prolongada no afecta únicamente a la organización internamente, sino que tiene consecuencias directas y medibles sobre los dos grupos de usuarios que dependen del servicio.

Impacto de una caída prolongada del portal web:

Desde la perspectiva de los candidatos, una caída del portal impediría el acceso a sus perfiles, la consulta de vacantes disponibles y el seguimiento de procesos de selección en curso. En un contexto donde muchas personas dependen activamente de la plataforma para encontrar empleo, una interrupción de más de 24 horas podría derivar en la pérdida de oportunidades laborales concretas y en la migración de usuarios hacia plataformas competidoras. Desde la perspectiva de las empresas clientes, la indisponibilidad del portal interrumpiría procesos de selección activos, retrasaría la publicación de nuevas vacantes y afectaría los compromisos de servicio acordados, lo que podría traducirse en pérdida de contratos y daño a la reputación comercial de la organización a nivel nacional.

Priorización de operaciones críticas durante una contingencia:

Ante una interrupción del portal web, la organización deberá priorizar la restauración de sus funciones en el siguiente orden de criticidad:

- Prioridad 1: restablecer el acceso a la base de datos de candidatos y vacantes activas, ya que son el núcleo del servicio.
- Prioridad 2: restablecer el portal web para candidatos y empresas clientes, garantizando la continuidad de los procesos de selección en curso.
- Prioridad 3: restablecer las funciones administrativas internas y las comunicaciones entre oficinas regionales.

Durante el tiempo que dure la contingencia, las oficinas regionales deberán activar procedimientos de atención presencial para los casos más urgentes, especialmente para candidatos con procesos de selección en etapa final o empresas con necesidades de contratación inmediata.

Protocolo de comunicación durante una contingencia:

La comunicación oportuna y transparente con los usuarios afectados es tan importante como la recuperación técnica del sistema. Una organización que no comunica durante una crisis genera desconfianza y acelera la pérdida de usuarios. Por esta razón, el plan de continuidad debe incluir un protocolo de comunicación estructurado en tres momentos:

- Comunicación inmediata — primeras 2 horas: notificar a candidatos y empresas clientes a través del correo electrónico registrado en la plataforma informando que se ha presentado una interrupción del servicio, que el equipo técnico está trabajando en su solución y que se enviará una actualización en un plazo definido. El mensaje debe ser claro, breve y evitar tecnicismos.
- Comunicación de seguimiento — cada 4 horas: enviar actualizaciones periódicas sobre el estado de la restauración, indicando el tiempo estimado de restablecimiento del servicio y las alternativas disponibles para los usuarios que requieran atención urgente, como la atención presencial en oficinas regionales.
- Comunicación de cierre — al restablecer el servicio: notificar el restablecimiento completo del portal, explicar brevemente la causa del incidente en términos comprensibles para el usuario general y comunicar las medidas adoptadas para evitar su recurrencia. Este mensaje cumple una función reputacional clave, ya que demuestra transparencia y responsabilidad institucional frente a los afectados.

La responsabilidad de ejecutar este protocolo de comunicación recae en la dirección general, con el apoyo del área comercial para la comunicación hacia empresas clientes y del personal de atención al usuario para la comunicación hacia candidatos. El administrador de TI designado será el responsable de proveer información técnica actualizada que permita alimentar cada comunicación con datos precisos sobre el estado real de la recuperación.

5.6 Indicadores de gestión

Para evaluar la efectividad del esquema de gestión de incidentes y continuidad, la organización deberá hacer seguimiento a los siguientes indicadores:

Indicador	Descripción	Meta sugerida
Tiempo de detección	Tiempo promedio entre la ocurrencia y la detección de un incidente	Menos de 2 horas
Tiempo de contención	Tiempo promedio entre la detección y la contención del incidente	Menos de 4 horas

Tiempo de recuperación	Tiempo promedio para restablecer la operación normal	Menos de 8 horas
Tasa de reincidencia	Porcentaje de incidentes que se repiten por la misma causa	Menos del 10%
Incidentes reportados vs. resueltos	Proporción de incidentes reportados que fueron gestionados formalmente	100%

6. Cultura Organizacional en Seguridad de la Información

6.1 La cultura de seguridad como pilar estratégico

La implementación de controles técnicos y políticas formales de seguridad constituye una condición necesaria pero no suficiente para proteger los activos de información de una organización. La experiencia en gestión de seguridad demuestra que la mayoría de los incidentes tienen como factor común el error humano, ya sea por desconocimiento, negligencia o falta de conciencia sobre los riesgos asociados al manejo de la información. Por esta razón, la construcción de una cultura organizacional orientada a la seguridad de la información es tan importante como cualquier control técnico implementado.

En el caso de la organización analizada, esta necesidad es especialmente evidente. Los incidentes registrados — ataques de phishing que encontraron receptividad en el personal, uso inadecuado de información por parte de empleados y el uso generalizado de canales informales para la gestión operativa — son manifestaciones directas de una cultura organizacional en la que la seguridad de la información no ha sido interiorizada como una responsabilidad compartida por todos los miembros de la empresa.

6.2 Diagnóstico de la cultura actual

Antes de diseñar un programa de cultura en seguridad, es necesario reconocer el punto de partida de la organización. Con base en el análisis desarrollado en las secciones anteriores, es posible identificar las siguientes características de la cultura organizacional actual en materia de seguridad:

Característica	**Situación actual**
Conocimiento sobre seguridad de la información	Bajo — no existen programas de formación formales

Percepción del riesgo por parte del personal	Baja — los incidentes no se reportan de manera sistemática
Cumplimiento de normas de seguridad	Inexistente — no hay políticas formales que cumplir
Uso de canales seguros de comunicación	Deficiente — predomina el uso de canales informales
Responsabilidad frente al manejo de datos	No definida — no hay roles ni responsabilidades claras
Liderazgo en seguridad desde la dirección	Ausente — no existe un referente interno en seguridad

6.3 Programa de concienciación y formación

El primer paso para transformar la cultura organizacional en materia de seguridad es garantizar que todo el personal comprenda por qué la seguridad de la información es importante, cuáles son los riesgos reales a los que está expuesta la organización y cuál es su rol individual en la protección de los activos de información. Para lograrlo, se propone el diseño e implementación de un programa de concienciación estructurado en tres niveles.

Nivel 1 — Formación básica obligatoria para todo el personal

Este nivel está dirigido a todos los empleados de la organización, independientemente de su cargo o área. Su objetivo es establecer un conocimiento mínimo común sobre seguridad de la información. Los temas por abordar incluyen:

- Qué es la seguridad de la información y por qué es responsabilidad de todos.
- Cómo identificar un correo de phishing o un intento de ingeniería social.
- Uso correcto del correo corporativo y prohibición de canales informales para gestión operativa.
- Manejo adecuado de contraseñas y accesos a sistemas.
- Qué hacer y a quién reportar ante un incidente o situación sospechosa.
- Obligaciones del personal frente a la Ley 1581 de 2012 y la protección de datos personales.

Esta formación deberá realizarse de manera obligatoria al momento de la vinculación de cada nuevo empleado y actualizarse anualmente para todo el personal.

Nivel 2 — Formación especializada por rol

Este nivel está dirigido a grupos específicos de empleados cuyas funciones implican un manejo más intensivo o sensible de la información. Incluye al personal de TI, al equipo comercial que gestiona la relación con empresas clientes, al personal de atención al usuario que accede a datos de candidatos y a los líderes regionales responsables de las oficinas en todo el país. La formación especializada profundiza en los riesgos específicos asociados a cada rol y en los controles y procedimientos que cada grupo debe aplicar en su trabajo diario.

Nivel 3 — Formación para la dirección y liderazgo

La cultura de seguridad no puede construirse desde abajo hacia arriba si no cuenta con el respaldo activo de la dirección. Este nivel está dirigido a los líderes y tomadores de decisiones de la organización, y tiene como objetivo que la alta dirección comprenda el valor estratégico de la seguridad de la información, las implicaciones legales y reputacionales de los incidentes, y su rol como promotores y garantes de una cultura organizacional segura.

6.4 Estrategias de refuerzo continuo

La formación puntual no es suficiente para consolidar una cultura de seguridad sostenible en el tiempo. Se requieren estrategias de refuerzo continuo que mantengan el tema vigente en el día a día de la organización. Entre las más efectivas para el contexto de la empresa analizada se proponen las siguientes:

- Simulacros de phishing: realizar envíos periódicos de correos de phishing simulados al personal para evaluar su nivel de alerta y reforzar la formación en quienes fallen en la prueba. Esta estrategia ha demostrado ser una de las más efectivas para reducir la tasa de éxito de ataques reales de ingeniería social.
- Comunicaciones internas de seguridad: publicar mensajes periódicos a través del correo corporativo con recordatorios, alertas sobre nuevas amenazas y buenas prácticas de seguridad adaptadas al contexto de la organización.
- Reconocimiento de buenas prácticas: establecer mecanismos de reconocimiento para empleados que reporten incidentes, identifiquen amenazas o demuestren comportamientos ejemplares en el manejo de la información. El reconocimiento positivo es un motivador más efectivo que la sanción para consolidar comportamientos seguros.
- Política de escritorio limpio: promover entre el personal el hábito de no dejar información sensible visible en sus puestos de trabajo, bloquear los equipos al ausentarse y no anotar contraseñas en lugares físicos accesibles.

6.5 Indicadores de cultura de seguridad

Para evaluar el avance en la transformación cultural, la organización deberá hacer seguimiento a indicadores que reflejen no solo el conocimiento del personal sino también sus comportamientos reales frente a la seguridad.

Indicador	Descripción	Meta sugerida
Cobertura de formación	Porcentaje del personal que completó la formación básica	100% anual
Tasa de detección en simulacros de phishing	Porcentaje de empleados que identifican correctamente un phishing simulado	Mayor al 85%
Incidentes reportados por el personal	Número de incidentes reportados voluntariamente por empleados	Incremento progresivo
Reincidencia en uso de canales informales	Casos identificados de uso de mensajería personal para gestión operativa	Reducción progresiva hasta cero
Satisfacción con los programas de formación	Evaluación del personal sobre la pertinencia y calidad de la formación recibida	Mayor al 80% de valoración positiva

6.6 Rol de la dirección en la consolidación de la cultura

La transformación cultural en materia de seguridad de la información requiere un compromiso visible y sostenido por parte de la alta dirección. Esto implica que los líderes de la organización no solo aprueben las políticas y los programas de formación, sino que los cumplan y los promuevan activamente en su comportamiento diario. Una dirección que utiliza canales informales para comunicar información sensible, que no exige el cumplimiento de las políticas de acceso o que no destina recursos para la formación del personal, envía un mensaje implícito que contradice cualquier esfuerzo por construir una cultura de seguridad sólida. En este sentido, el liderazgo en seguridad de la información debe entenderse como una responsabilidad estratégica de la dirección y no como una tarea delegable exclusivamente al área técnica.

6.7: Gestión del cambio y superación de resistencias

La implementación de una cultura de seguridad no es únicamente un proceso técnico ni formativo — es fundamentalmente un proceso de cambio organizacional. En la práctica, uno de los mayores obstáculos que enfrentan las organizaciones al intentar transformar sus hábitos de seguridad no es la falta de conocimiento sino la resistencia natural de las personas a abandonar prácticas que consideran cómodas, eficientes o inofensivas. En el caso de la organización analizada, el uso de aplicaciones de mensajería personal para la gestión operativa es un ejemplo claro de este fenómeno: los empleados no utilizan estos canales con intención de causar daño, sino porque son rápidos, familiares y funcionales para su trabajo diario. Pedirles que los abandonen sin ofrecer una alternativa igualmente ágil y sin explicar claramente el riesgo que implican generará resistencia, incumplimiento silencioso y, en el mejor de los casos, un cumplimiento superficial que no transforma el comportamiento real.

Estrategias para lograr compromiso real:

El compromiso genuino de los empleados frente al cambio cultural en seguridad no se obtiene únicamente a través de políticas y sanciones, sino a través de tres elementos fundamentales: comprensión, participación y experiencia positiva.

La comprensión implica que cada empleado entienda no solo qué debe hacer sino por qué importa. En lugar de comunicar las nuevas políticas como una lista de prohibiciones, la dirección deberá explicar en términos concretos y cercanos qué podría ocurrirle a la organización — y a cada empleado individualmente — si se materializa un incidente de seguridad. Un mensaje como "si nuestra base de datos de candidatos es robada, podemos enfrentar sanciones legales que pongan en riesgo la operación y los empleos de todos" genera más compromiso que una circular que prohíbe el uso de WhatsApp sin explicar el motivo.

La participación implica involucrar a los empleados en el proceso de cambio en lugar de imponérselo. Una estrategia efectiva es conformar un grupo de embajadores de seguridad, integrado por empleados voluntarios de diferentes áreas y oficinas regionales, que actúen como referentes internos del cambio, resuelvan dudas de sus compañeros y transmitan una visión positiva de las nuevas prácticas. Este enfoque es especialmente útil en una organización con presencia nacional, donde la dirección central no puede estar presente en cada oficina regional para supervisar y motivar el cambio directamente.

La experiencia positiva implica que el proceso de adopción de nuevas prácticas sea percibido como una mejora y no como una carga. Para lograrlo, la organización deberá garantizar que las herramientas corporativas que reemplazan los canales informales sean funcionales, accesibles desde dispositivos móviles y al menos tan ágiles

como las aplicaciones que se pretende sustituir. Si el correo corporativo tarda en cargar, no funciona bien en celular o resulta engorroso para comunicaciones rápidas, los empleados volverán inevitablemente a WhatsApp. La solución tecnológica debe estar lista antes de exigir el cambio de comportamiento.

Cómo enfrentar la resistencia al abandono de canales informales:

La resistencia al abandono del uso de mensajería personal es predecible y debe gestionarse de manera explícita. Se identifican tres tipos de resistencia frecuentes en este contexto y una estrategia de respuesta para cada uno:

- Resistencia por hábito: el empleado usa canales informales simplemente porque siempre lo ha hecho y no ve el problema. La respuesta más efectiva es la demostración práctica del riesgo, por ejemplo, a través de un simulacro o caso hipotético que ilustre cómo una conversación de WhatsApp con información de un candidato podría llegar a manos equivocadas. Ver el riesgo de forma concreta es más persuasivo que cualquier política escrita.
- Resistencia por conveniencia: el empleado reconoce el riesgo, pero considera que el canal informal es más práctico para su trabajo. La respuesta es eliminar la fricción del canal alternativo, habilitando una herramienta corporativa de mensajería interna que ofrezca la misma inmediatez que WhatsApp, pero bajo el control de la organización. Existen soluciones de bajo costo o gratuitas para empresas, como Microsoft Teams en su versión básica o Google Chat, que pueden integrarse fácilmente con el correo corporativo existente.
- Resistencia por desconfianza: el empleado percibe las nuevas políticas como un mecanismo de control o vigilancia por parte de la dirección. La respuesta es la transparencia: comunicar claramente que el objetivo de las políticas es proteger a la organización y a sus empleados, no monitorear conversaciones personales, y reforzar este mensaje con el ejemplo visible de los líderes que cumplen las mismas normas que exigen a sus equipos.

Métricas de avance en la gestión del cambio:

Para evaluar si el proceso de cambio cultural está generando resultados reales y no solo cumplimiento formal, la organización deberá hacer seguimiento a indicadores cualitativos además de los cuantitativos ya propuestos:

Indicador	Descripción	Meta sugerida

Percepción del cambio	Encuesta semestral sobre la percepción del personal frente a las nuevas políticas	Mejora progresiva en valoración positiva
Participación voluntaria	Número de empleados que se integran como embajadores de seguridad	Al menos uno por oficina regional
Reportes espontáneos de riesgo	Número de situaciones de riesgo reportadas voluntariamente por empleados sin que medie una obligación formal	Incremento sostenido trimestral
Reincidencia tras capacitación	Porcentaje de empleados que repiten comportamientos inseguros después de recibir formación	Reducción progresiva hasta menos del 5%

Conclusiones

El presente informe permitió desarrollar un análisis integral de la seguridad de la información en una organización dedicada a la intermediación laboral a escala nacional, identificando de manera estructurada sus activos de información, las amenazas y vulnerabilidades a las que está expuesta, los riesgos derivados de dicha exposición y las acciones necesarias para fortalecer su postura de seguridad.

La primera conclusión que se desprende del análisis es que la organización opera en un estado de vulnerabilidad significativa frente a la seguridad de la información. La ausencia de políticas formales documentadas, la inexistencia de un área de TI constituida como unidad formal y la falta de controles técnicos y administrativos básicos configuran un entorno en el que los riesgos identificados no solo son probables, sino que en varios casos ya se han materializado, como lo evidencian los incidentes de phishing, accesos no autorizados y uso inadecuado de información por parte de empleados registrados en la organización.

La segunda conclusión hace referencia al alto nivel de exposición legal al que se enfrenta la organización. Al gestionar datos personales de más de mil candidatos y quinientas empresas clientes sin contar con políticas de privacidad formales, mecanismos de autorización documentados ni un responsable designado para el tratamiento de datos, la organización incumple de manera activa los principios establecidos por la Ley 1581 de 2012. Esta situación la expone a sanciones por parte de la Superintendencia de Industria y Comercio y representa un riesgo reputacional que podría afectar la confianza de sus usuarios y clientes.

La tercera conclusión señala que el factor humano constituye el eslabón más débil en la cadena de seguridad de la organización. Los incidentes registrados tienen en común que pudieron haberse evitado o mitigado con personal capacitado y consciente de su rol en la protección de la información. La ausencia de programas de formación y la inexistencia de una cultura organizacional orientada a la seguridad amplifica el impacto de cualquier amenaza externa o interna, independientemente de los controles técnicos que se implementen.

La cuarta conclusión destaca que la organización cuenta con condiciones favorables para iniciar un proceso de mejora. Su infraestructura tecnológica basada en la

nube, su alcance nacional y el tamaño de su planta de personal son elementos que, correctamente gestionados, pueden convertirse en fortalezas. La implementación progresiva de las políticas, controles y programas propuestos en este informe permitiría a la organización avanzar hacia un nivel de madurez en seguridad alineado con los estándares de la ISO 27001 y el NIST Cybersecurity Framework, y en pleno cumplimiento de la normativa colombiana vigente.

Referencias

Agencia Española de Protección de Datos. (2021). Guía de análisis de riesgos para el tratamiento de datos personales. https://www.aepd.es/guias/guia-analisis-riesgo-rgpd.pdf

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Chicano Tejada, E. (2014). Gestión de incidentes de seguridad informática. IC Editorial.

Instituto Colombiano de Normas Técnicas y Certificación. (2013). NTC-ISO/IEC 27001: Tecnología de lac información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. ICONTEC.

Mitnick, K. D., y Simon, W. L. (2002). El arte de engañar: Controlando el elemento humano de la seguridad. Wiley Publishing.