TECHCORE.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión: 1.0

Código de documento: PO-GMG-2025-0002

Elaborado por: José Luis Robelo

Technology Core, S.A.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	***PO-GMG-2025-0002***
Versión:	2
Fecha de la versión:	31/07/25
Creado por:	Gerencia de Operaciones
Visto Bueno:	Quality Assurance
Aprobado por:	Gerencia General
Nivel de confidencialidad:	2

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
31/07/25	1	José Luis Robelo	Creación del documento / Versión inicial
10/10/25	2	Freddy Gómez	Actualización de los objetivos y comunicación de la política

CONTENIDO

1. SECCIÓN I – GENERALIDADES

1.1 Objetivo

Establecer las directrices para la protección de la información que los colaboradores y terceros deben cumplir con relación al acceso, uso y manejo de los activos de información de la compañía.

Proveer las disposiciones esenciales para asegurar la aplicación de medidas de protección a las herramientas tecnológicas e información del TechCore y lograr que esta sea integra, confidencial y pueda estar disponible cuando sea requerida para propósitos del negocio.

1.2 Alcance

La política aplica para todos los colaboradores del TechCore, prestadores de servicios, visitantes, contratistas y/o terceros que accedan a la información digital y recursos de tecnología de la compañía.

Esta política aplica a cualquier equipo de cómputo, dispositivos móviles como, tabletas, celulares y cualquier otro dispositivo de la corporación o personal, que sea conectado a la red interna de TechCore y/o cuando se acceda a información corporativa desde dichos dispositivos.

Esta política cubre el uso de los servicios de nube contratados por TechCore, información almacenada en nube, aplicaciones de nube donde se procesan y/o se hacen uso de los datos.

La política está disponible en la página web de la organización con acceso a todas las partes interesadas de TechCore, a su vez es compartida y explicada a todos los colaboradores de la organización con el fin de lograr su entendimiento.

1.3 Definiciones

Activo de Información: Son aquellos elementos que tienen valor para la organización, que contienen datos o información y que ante su afectación podría poner en riesgo algún proceso del negocio. Incluye pero no limitado a: registros, archivos, datos, facilidades de tecnología de la información, equipos (incluso los sistemas de computación personal), instalaciones y el software licenciado por la corporación.

Arquitectura de Seguridad: Configuraciones de seguridad definidas de acuerdo a la estructura tecnológica y procesal de los sistemas de información basados en buenas prácticas de seguridad y estándares de configuración.

Autenticar: Verificar que un ente comunicante (usuario, aplicación, dispositivo) es quien dice ser.

Base de Datos: Conjunto de datos relacionados en función de características específicas, que en su conjunto soportan el almacenamiento de la información del negocio y pueden ser accedidos a través de criterios de selección específicos.

Sistema Operativo: Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.

Contraseña (Password): Cadena arbitraria de caracteres alfanuméricos elegidos por un usuario o programa, usados para autenticar al usuario y prevenir el acceso no autorizado a su cuenta.

Confidencialidad: Cualidad de la información que garantiza que la misma sea accedida solamente por los usuarios autorizados. Su acceso por parte de personas no autorizadas podría causar un impacto negativo en la Organización.

Gestión de Cambio: Asegura que cualquier cambio introducido en el entorno de TI, es debidamente definido, evaluado y aprobado antes de su implementación, reducirá al mínimo la probabilidad de interrupción, errores y modificaciones no autorizadas.

Comité de Cambio: Es un grupo de personas que apoyan en la evaluación, priorización, autorización y programación de los cambios.

Cuentas de Usuarios: Identificador de Usuario dentro de los sistemas, cuyo responsable son colaboradores o personal externo de TechCore.

Cuentas Privilegiadas Usuario con niveles de acceso superiores a los normalmente asignados sobre un recurso de cómputo, que tiene bajo su responsabilidad la realización de tareas de configuración o procesos sensibles del negocio.

DMZ: una zona desmilitarizada (conocida también como DMZ, sigla en inglés de Demilitarized Zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna en el caso de que unos intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada**.**

Disponibilidad: Cualidad de la información que garantiza que la misma pueda ser accedida en el momento en que el negocio lo requiera. Si la información no se encuentra disponible cuando es requerida, podría resultar en una perdida financiera significativa o impacto negativo para la Organización.

Estándares: son un conjunto de reglas detalladas, que hacen mención específica de tecnologías, metodologías, procedimientos de implantación, y otros factores, resultantes de la aplicación de los lineamientos establecidos.

Factores de Autenticación: Técnica de verificación de identidad basada en dispositivos o información que sólo quien se autentica posea, sea o conozca.

Integridad: Cualidad de la información que garantiza que la misma no ha sido alterada, comprometiendo su exactitud y completitud, cuando es usada para soportar los procesos de negocio de la organización.

Política de Ciberseguridad: Enunciados de alto nivel que establecen directrices que regulan la forma como una organización maneja y protege su información para mitigar los riesgos a los que se encuentran expuesta, producto de la operación y gestión normal del negocio. Estos enunciados son de carácter general y por lo tanto, deben estar diseñados para un horizonte de largo plazo

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Software Malicioso o Malware: Es un tipo de software que tiene como objetivo infiltrarse o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario; el término procede del inglés malicious software.

Programa de Concientización: Plan que contiene una serie de actividades a realizar para retroalimentar a todos los colaboradores en relación con las políticas y buenas prácticas de seguridad de la información que deben ser adaptadas en la organización. Capacita a los usuarios sobre las posibles amenazas a la información y cómo evitar situaciones que puedan poner en riesgo los datos de la organización.

Propietario de Información: Individuo o unidad de la corporación responsable del activo de información, que tiene el compromiso de clasificarla, protegerla y tomar decisiones con respecto a su uso durante la operación del negocio.

Terceras partes / Terceros: Asociados de negocio, clientes o proveedores con los cuales existe un intercambio de información, o relación comercial con TechCore.

- Bluestone Resources Inc.: Records Management Policy
- Política de Seguridad de la Información
- Política de Clasificación de la Información

1.4 Roles y Responsabilidades

I. **Auditoría:** Responsable de proporcionar una visión independiente del cumplimiento de la política.

II. **Áreas de Tecnología de la Información:** Equipos responsables de apoyar en las configuraciones e implementaciones de lineamientos técnicos en los sistemas e infraestructura de red con el objetivo de enforzar los preceptos dictados en esta política.

III. **CISO:** Responsable de promover el cumplimiento de la política de ciberseguridad. Somete a consideración del Comité de Ciberseguridad recomendaciones de cambios a la política, a algunos de sus elementos; así como impulsar los proyectos relacionados con Ciberseguridad.

IV. **Colaborador:** Cumplir con lo establecido en esta política. Es responsable del uso correcto de los activos lógicos y físicos asignados.

V. **Comité de Ciberseguridad:** Proponer mejoras, realizar actualizaciones sobre la Política de Ciberseguridad y velar por la ejecución del plan de cumplimiento de lo establecido en la misma. Gestionar de forma transversal las brechas de cumplimiento sobre esta política. Diseñar e implementar un programa de concientización de ciberseguridad que apalanquen el cumplimiento de la política.

VI. **Comité Directivo:** Patrocinadores y promotores de las estrategias, iniciativas y normatividad relacionadas con ciberseguridad.

VII. **Comunicación Interna:** Difundir a través de los medios de comunicación corporativos más idóneos los aspectos de esta política que sean enmarcados dentro del programa de concientización

VIII. **Custodio de la Información:** Son los responsables de la administración de los activos de información de acuerdo con las especificaciones de su Propietario. Ejecutan este rol las áreas de Tecnología y proveedores que tienen acceso a los activos de la información.

IX. **Director Senior de TI:** Responsable de impulsar en conjunto con el CISO las definición, implementación y cumplimiento de la política de ciberseguridad además de lograr su aprobación a nivel de la junta directiva.

X. **Equipos de Ciberseguridad:** Equipos responsables de las tareas de operación y de llevar a cabo los proyectos de ciberseguridad que apoyan en el cumplimento de esta política.

I. **Junta Directiva / Comité Ejecutivos:** Aprobar las Política de Ciberseguridad. Es el responsable de asignar los recursos necesarios para el cumplimiento de los objetivos del negocio tomando en cuenta el ámbito de ciberseguridad.

XI. **Legal:** Validar y revisar los requisitos de ciberseguridad en los contratos con proveedores y terceros.(ej. clausulado para aspectos de confidencialidad de información y propiedad intelectual).

XII. **Recursos Humanos:** Comunicar al personal sobre sus obligaciones con respecto a la política de ciberseguridad antes de su contratación y durante la relación laboral.

XIII. **UCMI:** Colabora de forma activa con el programa de concientización apoyando con el objetivo de elevar el nivel de cultura de ciberseguridad en la corporación mediante el aprovechamiento de sus mecanismos y herramientas de enseñanza.

XIV. **Terceros:** Cumplir con lo establecido en esta política de acuerdo a los accesos lógicos y físicos otorgados durante el tiempo de ejecución de los servicios o productos contratados.

XV. **Propietarios de la Información:** Responsable de definir los requerimientos de seguridad para lograr que la información obtenga el nivel adecuado de protección. Autoriza el acceso a los sistemas considerando la clasificación de la información.

XVI. **Usuarios de la Información:** Cumplir con la política de ciberseguridad utilizando los activos de información sólo para el propósito autorizado mediante una conducta ejemplar que evite la divulgación o uso inapropiado de la información.

1.5 Compromiso de la Alta Dirección

La Alta Dirección de TechCore se compromete a:

- Proteger los activos de información frente a amenazas internas y externas, las cuales se establecen el documento de Contexto de Organización
- Cumplir con los requisitos legales, regulatorios y contractuales aplicables, incluyendo la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley 8968).
- Implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022.
- Apoyar la capacitación y concientización del personal sobre seguridad de la información y, cuando aplique, a las partes interesadas externas de la organización.
- Promover una cultura de seguridad adecuada al entorno de teletrabajo.

1.6 Objetivos de Seguridad de la Información

TechCore se compromete a cumplir con los siguientes principios:

I. Confidencialidad: La información será accesible solo a las personas autorizadas.
II. Integridad: La información será precisa, completa y protegida contra modificaciones no autorizadas.
III. Disponibilidad: La información estará disponible cuando sea requerida por los usuarios autorizados.

Además de los objetivos anteriormente mencionados, TechCore cuenta con los siguientes principios, que se encuentran desarrollados en el Plan Estratégico de la organización:

I. Garantizar la confidencialidad, integridad y disponibilidad de la información corporativa y de los clientes.
II. Asegurar el cumplimiento de requisitos legales, normativos y contractuales aplicables en materia de seguridad de la información.
III. Fortalecer la cultura organizacional de seguridad y resiliencia ante incidentes.

1.7 Revisión y Mejora Continua

La presente política será revisada al menos una vez al año en la reunión anual de Revisión por la Dirección o cuando ocurran cambios significativos en los riesgos, procesos o tecnologías utilizadas. Cualquier modificación será aprobada por la Alta Dirección.

2. SECCIÓN II POLITICAS

2.1 CLASIFICACIÓN DE INFORMACIÓN

2.1.1 La información en la corporación se clasifica de acuerdo con los siguientes niveles:

I. **Confidencial**: Es la información más sensible o de mayor valor para la organización, y puede traer impacto severo a la corporación si la misma es revelada sin autorización, alterada inapropiadamente o no se encuentre disponible para el personal o procesos que la requieren. Deberá mantenerse dentro de la organización utilizada por áreas específicas y podría estar regulada por acuerdos legales en ocasiones. El impacto puede comprender desde cuantiosas pérdidas monetarias, interrupción de las operaciones, hasta daños a la imagen de la corporación o la pérdida de un secreto industrial.

II. **Interna:** Toda información que puede traer un impacto **moderado** a la corporación si la misma es revelada sin autorización, alterada inapropiadamente o no se encuentre disponible para el personal o procesos que la requieren. Deberá

mantenerse dentro de la corporación y sin disponibilidad externa, a excepción de terceros involucrados con previa autorización del responsable quienes deberán estar comprometidos en no divulgar la misma. El impacto puede comprender desde interrupción mínima de las operaciones, tiempos moderados para su recuperación hasta afectaciones a algunos activos.

III. **Pública:** Toda información que no impacta a la corporación, accionistas, sus colaboradores ni a clientes, si la misma es revelada sin autorización. Agrupa información explícitamente aprobada para ser divulgada con acceso público, debido a que no constituye riesgo. La información es comúnmente conocida y utilizada por cualquier persona o empleado, y no compromete las operaciones de la organización.

2.1.2 De acuerdo con el nivel de clasificación de la información se deben implementar mecanismos de control y protección adecuados.

2.1.3 El nivel de clasificación de la información es proporcionado por su propietario.

2.2 CONTROL DE ACCESOS

2.2.1 CONTROL DE ACCESO DE USUARIOS FINALES

2.2.1.1 Todo acceso a los sistemas de la corporación debe quedar autorizado y registrado.

2.2.1.2 Los derechos de acceso otorgados deben limitarse a lo que el usuario necesita para el desempeño de sus labores. Si existen modificaciones en las posiciones de trabajo los derechos de acceso asociados también deben modificarse.

2.2.1.3 Se debe aplicar una identificación única a las cuentas de usuarios en los sistemas que permiten asociar a los propietarios de las cuentas con sus respectivas actividades y hacerlos responsables de sus acciones. Si por razones operativas o del negocio es necesario el uso de cuentas compartidas, éstas deben ser debidamente autorizadas y documentadas.

2.2.1.4 La responsabilidad del uso de las cuentas de usuario y contraseña es solamente del que las posee. El usuario es responsable de la confidencialidad de la cuenta de usuario y contraseña. La contraseña no debe ser compartida por ningún medio, salvo excepción con aprobación de las áreas de RH y/o Jurídico.

2.2.2 CONTROL DE ACCESOS DE USUARIOS PRIVILEGIADOS

2.2.2.1 Los colaboradores cuyas responsabilidades incluyen el acceso con funciones de administrador a infraestructura de tecnología, servicios o aplicativos, deberán contar con una cuenta adicional para la ejecución de las tareas de administración asignadas. Dichas cuentas son las denominadas Cuentas Privilegiadas.

2.2.2.2 El acceso mediante cuentas privilegiadas deberá ser reservado sólo para el personal que, por sus funciones, de administración, seguridad o monitoreo de sistemas, justifique la necesidad de tener dicho tipo de acceso.

2.2.2.3 Se debe establecer un control de las cuentas de usuarios con acceso privilegiado, con el objetivo de minimizar el riesgo asociado a la utilización de estos.

2.2.2.4 El acceso de los identificadores de cuentas privilegiadas que vienen por defecto en los recursos de cómputo debe ser restringido o desactivado.

2.2.3 AUTENTICACIÓN

2.2.3.1 Se debe asegurar que todos los sistemas y aplicaciones requieran al menos un factor de autenticación para corroborar la identidad del usuario.

2.2.3.2 Dependiendo del valor de la información y del nivel de riesgo a la que se encuentra expuesta, TechCore definirá e implantará las herramientas y medios de identificación y autenticación apropiados, los cuales deberán estar habilitados en los recursos de información establecidos por la organización, de manera de restringir el acceso para los diferentes roles y responsabilidades del personal.

2.2.3.3 Antes de reestablecer las contraseñas para la autenticación del usuario se deben cumplir los procedimientos para verificar la identidad del usuario.

2.2.3.4 La contraseña por defecto que vienen en los productos de fabricantes se debe modificar después de la instalación del activo (equipo de cómputo, servidores, SO, BD etc.).

2.3 SEGURIDAD DE OPERACIONES Y COMUNICACIONES

2.3.1 SEPARACIÓN DE AMBIENTES

2.3.1.1 Los ambientes de desarrollo, calidad y producción de las distintas plataformas tecnológicas deben estar separados. Por lo tanto, la corporación debe proveer los recursos necesarios para contar con ambientes de desarrollo y calidad, separados del ambiente de producción, ya sea en plataformas tecnológicas diferentes o con un manejo de librerías separadas con controles de acceso basados en los factores de autenticación permitidos por la corporación.

2.3.1.2 Todo cambio que ser realice entre estos ambientes deben ser realizados bajo un estricto control por medio del proceso establecido para la gestión de cambios, y los responsables para su ejecución deben estar claramente asignados y definidos.

2.3.1.3 El personal de las áreas de desarrollo de sistemas no debe modificar o acceder a la información de los ambientes de producción sin contar con la autorización de los Propietarios.

2.3.2 ESTÁNDARES SEGUROS DE CONFIGURACIÓN

2.3.2.1 Se debe implementar los lineamientos de configuraciones de seguridad mínimas requeridas sobre la infraestructura tecnológica de TechCore. Esto incluye seguridad en servidores, bases de datos y sistemas operativos. Se debe asegurar que todos los componentes tengan las últimas actualizaciones, se habiliten únicamente los puertos necesarios para realizar su función, entre otros parámetros que garanticen la seguridad de la infraestructura de TechCore.

2.3.3 MONITOREO DE SEGURIDAD

2.3.3.1 Se deben implementar un monitoreo constante de los recursos tecnológicos, con herramientas, para detectar con antelación o bien en el menor tiempo posible cualquier evento para garantizar la seguridad y la continuidad de las operaciones.

2.3.3.2 Se debe establecer métodos de monitoreo continuo de las cuentas privilegiadas, a fin de evitar abusos por acceso a data o información confidencial.

2.3.3.3 Se revisarán periódicamente los resultados obtenidos de los procesos de monitoreo realizados en los diferentes sistemas.

2.3.3.4 Las alertas de seguridad generadas por las herramientas y/o servicios de monitoreo deben ser validados y atendidos oportunamente para prevenir anomalías que puedan afectar la arquitectura tecnológica de la corporación.

2.3.4 SEGURIDAD EN REDES

2.3.4.1 **Políticas Generales:**

2.3.4.1.1 Se debe implementar controles que permitan asegurar el manejo de los datos en la red y la protección de los servicios compartidos frente a accesos no autorizados.

2.3.4.1.2 Se debe evaluar como posible mecanismo de control la segmentación de redes dentro de la corporación, agrupando lógicamente los recursos de cómputo de acuerdo con la confidencialidad de la información y las necesidades del negocio.

2.3.4.1.3 Se debe considerar mecanismos de cifrado robusto para la transmisión de información confidencial.

2.3.4.1.4 Las redes de comunicación deben considerar los controles de acceso que limiten la intercepción no autorizada de datos y el acceso a recursos restringidos.

2.3.4.1.5 Las transferencias de datos y archivos hacia redes externas incluida Internet, deben ser realizadas únicamente cuando exista una razón justificada de negocio, y dependiendo del nivel de clasificación e información trasmitida se debe considerar los mecanismos de protección de seguridad apropiados.

2.3.4.1.6 La operación de la red de comunicaciones deberá contar con funciones activas de monitoreo y generación de alertas de su capacidad.

2.3.4.2 **REDES INALÁMBRICAS**

2.3.4.2.1 Se deben establecer mecanismos y controles de seguridad que restrinjan el acceso a la red inalámbricas por parte de usuarios no autorizados.

2.3.4.2.2 En caso de presenciarse ingresos no autorizados a la red inalámbrica, se podrá proceder sin previo aviso a la desactivación del dispositivo de conexión (Access Point) al cual se ingresó sin autorización,

pudiendo quedar sin comunicación aquellos usuarios autorizados conectados al mismo.

2.3.5 SEGURIDAD PERIMETRAL

2.3.5.1 Deben definirse zonas de seguridad para controlar el acceso a redes.

2.3.5.2 Todo el tráfico entrante desde Internet debe estar bloqueado y habilitado únicamente para zonas específicas dentro de la red de la corporación, tipo zonas desmilitarizadas(DMZ).

2.3.5.3 Todo el tráfico saliente hacia internet debe estar restringido y habilitado únicamente para usuarios autenticados y autorizados.

2.3.5.4 Todo tráfico saliente de navegación debe ser filtrada a través de un sistema de filtrado de contenido.

2.3.6 SEGURIDAD DEL CORREO

2.3.6.1 El correo electrónico a nivel corporativo debe contar con mecanismos de seguridad mínimos, como por ejemplo, pero no limitado a antispam, inspección y análisis sobre los adjuntos y/o enlaces antes que el usuario pueda acceder a ellos.

2.3.7 SEGURIDAD EN INTERNET

2.3.7.1 El acceso a Internet corporativo será habilitado de acuerdo a las necesidades concernientes al puesto de trabajo de cada colaborador.

2.3.7.2 El uso de Internet corporativo deberá ser monitoreado constantemente con el objetivo de medir el consumo y podrán crearse controles adicionales para los usuarios con acceso a Internet que presenten un comportamiento sospechoso o que en forma comprobada pongan en riesgo la seguridad.

2.3.8 SEGURIDAD EN SERVIDORES WEB CRÍTICOS

2.3.8.1 Deberán contar con todas las actualizaciones de seguridad que apliquen para estar adecuadamente protegido.

2.3.8.2 Deberán generarse los procesos periódicos de respaldo del contenido de los servidores web.

2.3.8.3 Serán sujetos a evaluación y posible actualización constante sobre los mecanismos de seguridad acorde a las últimas tendencias tecnológicas que garanticen la autenticidad, la integridad y la confidencialidad de la información.

2.3.8.4 Se mantendrá un histórico de las actividades realizadas por los usuarios a través de Internet, a fin de disponer de la información pertinente para efectuar seguimientos y auditorias en caso de ser necesario.

2.3.9 CIFRADO DE INFORMACIÓN

2.3.9.1 Se debe considerar mecanismos de cifrado robusto para la información confidencial tanto en los procesos de trasmisión como en su almacenamiento.

2.3.9.2 Para asegurar la confidencialidad, autenticidad e integridad de la información, la corporación contará con procedimientos y controles para el uso de criptografía, tomando en consideración al menos lo siguiente:

i Utilizar mecanismos de protección criptográfica que cuenten con respaldo internacional y seleccionados según las buenas prácticas internacionales.

ii No utilizar mecanismos de protección criptográfica inseguros u obsoletos.

2.3.10 DESTRUCCIÓN DE DATOS

2.3.10.1 La información confidencial o de uso Interno de la corporación debe ser destruida en forma segura, cuando pierda su vigencia.

2.3.10.2 Cuando un recurso de cómputo va a ser dado a cambio, enviado a servicio o desechado, la información almacenada debe ser destruida conforme los métodos aprobados que se establezcan. Debe tenerse en cuenta el borrado de discos duros, o el borrado (por ejemplo reescritura con ceros binarios) de cualquier medio de almacenamiento que este incluido en el recurso de cómputo.

2.3.10.3 Debe asegurarse que la retención de datos aplique tanto a medios físicos como digitales, incluyendo respaldos, sistemas de almacenamiento y dispositivos portátiles, garantizando siempre la confidencialidad, integridad y disponibilidad de la información durante todo el ciclo de vida.

2.3.10.4 La eliminación lógica deberá realizarse mediante herramientas de borrado seguro que impidan la recuperación de la información. La destrucción física, cuando corresponda, deberá realizarse a través de métodos

irreversibles como trituración, desmagnetización o incineración, según el tipo de soporte.

2.3.10.5 Todo proceso de eliminación o destrucción de datos deberá quedar documentado en un Acta de Destrucción, que indique fecha, responsable, método aplicado y, de ser el caso, el proveedor externo que participó en el procedimiento.

2.3.10.6 La responsabilidad de garantizar la correcta eliminación o destrucción recae en los responsables de los activos de información, bajo supervisión del área de Seguridad de la Información. El incumplimiento de esta política será considerado una falta grave y podrá derivar en medidas disciplinarias conforme a la normativa vigente.

2.3.10.7 La presente política será revisada al menos una vez al año, o antes si se presentan cambios normativos, regulatorios o tecnológicos que así lo requieran.

2.4 CONTROL DE CAMBIOS

2.4.1 Implementar un proceso debidamente documentado de gestión de cambios y que contemple al menos, el establecimiento de controles en las pruebas de verificación y calidad, autorización, registro, procedimientos de regresión.

2.4.2 Todos los cambios a recursos informáticos, tales como: infraestructura de tecnologías de la información, sistemas de información, bases de datos, servicios de tecnología de información y su respectiva documentación deben seguir los procedimientos de gestión de cambios vigentes.

2.4.3 Debe designarse un Comité de Cambios cuyo objetivo será la evaluación, priorización, autorización y programación de los cambios cuya periodicidad de sesiones y lineamiento estarán dictados de acuerdo con un procedimiento definido.

2.4.4 Se debe designar una Comité de Cambios, la cual tendrá las siguientes responsabilidades:

I. Reunirse cuando la situación lo amerite para revisar los requerimientos de cambios y asegurarse así que las revisiones y la debida comunicación de los cambios sea satisfactoria y adecuada.

II. Revisar los requerimientos para detectar fallas potenciales que incluyan, pero no se limitan a: insuficiente planificación, inadecuados planes de contingencia, horas y fechas que impacten negativamente en algún proceso esencial del negocio como cierres mensuales y/o

anuales, o si los recursos para el cambio no son los adecuados, y tomar así la decisión de permitir, demorar o denegar el requerimiento.

III. Todos los cambios normales, estándar y de emergencia deben comunicarse en la reunión de la Comisión de Gestión de Cambios.

2.4.5 Los cambios deben clasificarse en tres tipos: cambios estándar, que son rutinarios y de bajo riesgo; cambios normales, que requieren un análisis de impacto, plan de pruebas y autorización formal; y cambios de emergencia, que deben aplicarse de forma inmediata para restaurar la continuidad de los servicios, pero que deben ser revisados posteriormente por el Comité de Cambios.

2.4.6 Cada cambio debe contar con una solicitud formal que incluya su descripción, el motivo, los sistemas o servicios afectados, el análisis de impacto, los riesgos identificados, los recursos necesarios, el plan de pruebas, así como un plan de reversión en caso de falla. Dichas solicitudes deben registrarse en la herramienta oficial de gestión de cambios para garantizar trazabilidad y evidencia del ciclo de vida del cambio.

2.4.7 Después de la implementación de un cambio, debe realizarse una revisión posterior (post-implementación) para confirmar que este fue exitoso, identificar posibles fallas no previstas y documentar las lecciones aprendidas que permitan mejorar el proceso.

2.4.8 La comunicación de los cambios debe ser clara y oportuna hacia los usuarios y áreas impactadas, procurando que estos se ejecuten en horarios y condiciones que minimicen el impacto en la operación.

2.4.9 Todos los colaboradores involucrados en la solicitud, aprobación, ejecución o revisión de cambios son responsables de cumplir con este procedimiento. El incumplimiento de la política de gestión de cambios será considerado una falta grave y podrá derivar en sanciones disciplinarias conforme al Reglamento Interno de Trabajo y la normativa vigente.

2.4.10 La política de gestión de cambios deberá revisarse al menos una vez al año, o antes si existen cambios normativos, tecnológicos o de negocio que lo requieran, con el fin de mantener su vigencia y efectividad.

2.5 RESPALDOS Y RESTAURACIÓN

2.5.1 CREACIÓN DE COPIAS DE SEGURIDAD

2.5.1.1 Se establecerán procedimientos para la realización de respaldos que contemplen copias de la información, programas, aplicaciones,

documentación, bases de datos, entre otros; incluyendo los procedimientos de recuperación del sistema y de la información de manera separada e independiente.

2.5.1.2 Se determinarán períodos de conservación de la información en las copias de respaldo durante los plazos que sean definidos según las regulaciones establecidas por entes supervisores o legales y las necesidades de la Corporación, determinadas por el propietario de la información y el administrador del sistema.

2.5.2 **PRUEBAS DE RESTAURACIÓN**

2.5.2.1 Los respaldos de la información deben ser probados periódicamente mediante la implementación del proceso de recuperación de datos definido por las áreas responsables verificando que todos los datos han sido restablecidos satisfactoriamente.

2.5.2.2 Se deben probar las copias de seguridad y los registros de las pruebas realizadas deben quedar documentados.

2.6 PROTECCCIÓN CONTRA SOFTWARE MALICIOSO

2.6.1 Todos los equipos de cómputo servidores y estaciones de trabajo, deben contar con la herramienta de protección de software malicioso, previamente instalada.

2.6.2 El colaborador no debe deshabilitar bajo ningún concepto la protección contra software malicioso.

2.6.3 Los usuarios deben tener acceso restringido a modificar los parámetros de configuración, solamente podrá ser ajustado/modificado por un administrador autorizado.

2.6.4 Los usuarios no deben desinstalar la protección contra software malicioso, ni instalar herramientas diferentes a las establecidas por TechCore.

2.6.5 Reportar de manera inmediata al área de seguridad de la información cualquier anomalía identificada, a través de la mesa de servicio

2.3 POLÍTICAS DE SEGURIDAD CON TERCEROS

2.6.6 Los riesgos de seguridad relacionados con proveedores y socios se identifican durante el proceso de evaluación de riesgos. Durante esta evaluación, se debe tener especial cuidado para identificar riesgos relacionados con tecnología de la información y comunicación, como también riesgos relacionados con la cadena de suministros de productos y/o servicios.

2.6.7 Se debe realizar un análisis de cumplimiento de buenas prácticas de seguridad de la información por medio de un cuestionario de solicitud de información solicitado en conjunto con toda la información y documentación requerida para el proceso de alta o actualización de proveedores definida por el área de abastecimiento.

2.6.8 Todo proveedor debe firmar un acuerdo de confidencialidad y contrato de servicios.

2.7 SEGURIDAD DE SERVICIOS EN LA NUBE

2.7.1 Todo contrato de servicios en la nube debe ser verificado y autorizado por la Dirección de TI.

2.7.2 Se debe definir un control de requisitos mínimos de seguridad que debe cumplir el proveedor de servicios en la nube.

2.7.3 La Dirección de TI debe proporcionar un punto de contacto principal para el proveedor responsable de administrar la relación, el Acuerdo de nivel de servicio (SLA) y garantizar que el proveedor cumpla con todos los términos del contrato.

2.7.4 Revisión periódica del personal de los proveedores de servicios en la nube autorizados que trabajan en el contrato y los servicios realizados por cada uno.

2.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

2.8.1 Se deberá garantizar que los aspectos de seguridad de la información sean contemplados en forma adecuada en el proceso de adquisición, desarrollo y mantenimiento de sistemas de información. Esto apegado a una metodología para gestionar el ciclo de vida del software, en base a las buenas prácticas internacionales en esta materia.

2.8.2 Toda solución tecnológica que se implante en la corporación debe haber ser construida de acuerdo con una metodología de desarrollo y mantenimiento de sistemas que considere los requerimientos de Seguridad de la Información, durante todo su ciclo de vida, desde el diseño hasta la puesta en operación.

2.8.3 Se deberán contemplar controles de seguridad en todo lo que se refiere a generación del dato, ingreso del dato, procesamiento, almacenamiento, emisión de reportes y consultas, a objeto de asegurar la integridad y confidencialidad de la información

2.8.4 Cuando los desarrollos sean realizados por terceros que empleen, o se adquiera software o soluciones de mercado, deben tenerse en cuenta los

mismos requerimientos de Seguridad y estándares establecidos por la corporación. Es necesario exigir al proveedor la aplicación de los mismos, e incluir los elementos correspondientes en los contratos o acuerdos que se formalicen.

2.8.5 Los ambientes de desarrollo, pruebas y producción deben estar perfectamente delimitados, existiendo una segregación de funciones entre las responsabilidades de desarrollo, pruebas, implantación y puesta en producción, todo esto complementado con un estricto control de versiones de los sistemas a ser implantados.

2.8.6 En adición a los controles a ser incluidos durante la implantación, cualquier cambio que se efectúe en la solución una vez operativa, deberá ser manejado de acuerdo con los procedimientos establecidos para tal efecto por la institución (Gestión de Cambio), verificando que los controles de seguridad hayan sido efectivamente incluidos y que se mantengan activos y en correcto funcionamiento.

2.9 GESTIÓN DE PARCHES Y VULNERABILIDADES

2.9.1 Se debe contar con controles y procedimientos que considere al menos los siguientes aspectos:

I. La implementación de un proceso de análisis, monitoreo y evaluación de la exposición de las vulnerabilidades de los sistemas críticos, para la implementación de mitigantes y gestión del riesgo residual.

II. La implantación de las actualizaciones de seguridad correspondientes y/o medidas mitigantes, conforme a los procesos operativos de la corporación.

2.10 CAPACITACIÓN Y CONCIENTIZACIÓN

2.10.1 Se debe desarrollar un plan de concientización que enfatice la importancia del Modelo de Seguridad de la Información y su contribución al logro de los objetivos del negocio.

2.10.2 Las campañas de concientización deben tener como objetivo impactar sobre el comportamiento de los colaboradores de la corporación, deben ser sencillas y prácticas utilizando ejemplos cotidianos con consecuencias reales.

2.10.3 La educación de los colaboradores de la corporación debe ser un sistema progresivo que incluya componentes tanto de concientización como de entrenamiento y debe tener como objetivo asegurar que los usuarios de todos

los niveles tengan los conocimientos y competencias suficientes para desempeñar sus roles dentro de la estrategia de seguridad.

2.10.4 Las presentaciones de concientización deben estar destinadas a permitir que las personas reconozcan los problemas de seguridad de TI y respondan en consecuencia.

2.10.5 Las necesidades de capacitación y concientización pueden determinarse considerando lo siguiente:

- Ejemplos cotidianos con consecuencias reales
- Entrevistas con grupos clave
- Cambio en políticas, normativas o procedimientos
- Encuestas corporativas
- Verificando el comportamiento general de los usuarios respecto a temas específicos
- Incidentes más comunes de seguridad
- Tendencias en el campo de seguridad

2.10.6 La priorización de los cursos o campañas de concientización debe realizarse con base en la disponibilidad de recursos, impacto en la corporación, necesidades críticas para un proyecto específico, brechas actuales de la estrategia de seguridad.

2.10.7 Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.

2.11 DEL USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

2.11.1 RESPECTO A LOS DISPOSITIVOS PROPIEDAD DE LA CORPORACIÓN

2.11.1.1 Los activos de información solamente pueden ser utilizados a fines de satisfacer las necesidades de la operación del negocio con el objetivo de ejecutar tareas vinculadas con la organización.

2.11.1.2 Cada activo de información tiene designado un propietario en el inventario de activos. El propietario del activo es el responsable de la

confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

2.11.2 **RESPECTO AL USO DE LOS DISPOSITIVOS PERSONALES**

2.11.2.1 El uso de Dispositivos Personales para acceder a información de TechCore, no es una práctica estándar de la corporación, y por consiguiente serán tratadas como casos excepcionales que deben quedar debidamente autorizados, mínimo a nivel de Dirección Senior justificado bajo una clara necesidad del negocio.

2.11.2.2 En los casos que sea estrictamente necesario el uso de dispositivos personales para acceder a los recursos y servicios de la corporación, queda entendido:

I. Todos los datos de la corporación que sean almacenados, transferidos o procesados en dispositivos personales siguen perteneciendo a TechCore, y la corporación mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo, y por consiguiente puede tomar acciones para eliminar la información de dichos dispositivos cuando así lo considere necesario.

II. Los dispositivos tienen que cumplir con los controles de seguridad que establezca la corporación

2.11.3 **RESPECTO AL TELETRABAJO**

2.11.3.1 Se debe establecer mecanismos que garanticen la seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se va a acceder y transmitir a través del enlace de comunicación, así como la sensibilidad de los sistemas de la corporación.

2.11.3.2 Mientras los activos de información (equipos de cómputo, celulares, tokens, entre otros.) asignados a los colaboradores permanezcan fuera de la organización, el cuidado, protección y uso adecuado de los mismos, queda bajo la entera responsabilidad del colaborador.

2.11.3.3 Los activos de información entregados a los colaboradores y que será utilizados para teletrabajo puede ser utilizados únicamente con fines laborales

2.11.3.4 Los colaboradores deben hacer uso de redes inalámbricas (WIFI) conocidas y que solicite contraseña o algún otro factor de autenticación de

seguridad para su conexión. Se debe evitar conexiones a redes inalámbricas públicas que requieran algún tipo de información personal y/o que pongan en riesgo la información institucional.

2.11.4 RESPECTO AL USO DEL CORREO ELECTRÓNICO

2.11.4.1 La cuenta de correo electrónico es de uso personal e intransferible, siendo responsabilidad del usuario salvaguardar el acceso a la información que reciba o envíe.

2.11.4.2 La cuenta de correo electrónico se puede utilizar únicamente para el manejo de la información de la corporación y no de carácter personal.

2.11.4.3 Los mensajes compartidos por correo corporativo son propiedad de TechCore por lo que los mismos pueden ser revisados en cualquier momento con el propósito de confirmar cumplimiento.

2.11.4.4 Cualquier usuario de cuenta de correo electrónico corporativo deberá cumplir con los siguientes lineamientos:

I. Está prohibido el uso de lenguaje inapropiado incluyendo, pero no limitado a discriminación, groserías, opiniones políticas, soez, sexuales, violencia entre otros.

II. Identificar la etiqueta del mensaje dada su relevancia: alta, baja o normal.

III. Los archivos adjuntos de alto volumen deben enviarse de manera comprimida o hacerse disponibles a través de folders accesibles desde la red.

IV. En caso de duda del destinatario o fuente de algún correo electrónico se debe reportar el caso a la mesa de servicio de TI.

V. Identificar claramente al destinatario y limitar el número de personas copiadas en el mensaje.

VI. Evitar el uso de destinatarios ocultos.

VII. Redactar los mensajes de manera clara, concisa y usando un lenguaje profesional y de negocio.

VIII. Identificar de manera clara y concisa el asunto del mensaje, haciendo referencia al contenido de este.

IX. En cada mensaje, hacer referencia a un único asunto

2.11.5 RESPECTO AL USO DE LAS REDES INALÁMBRICAS

2.11.5.1 Todos los equipos configurados para conexiones inalámbricas deberán poseer medidas de seguridad activas y actualizadas (antimalware, actualizaciones, entre otros).

2.11.5.2 El usuario a quien se le conceda el acceso a la red inalámbrica corporativa se compromete a hacer buen uso de esta.

2.11.5.3 Se debe evitar conectarse a redes Wi-Fi públicas y gratuitas ya que son menos seguras y más propensas a sufrir accesos no deseados y ataques.

2.11.6 RESPECTO AL USO DE INTERNET CORPORATIVO

2.11.6.1 El acceso a Internet es una herramienta laboral que apoya la función del día a día, por consiguiente, está restringido el acceso a sitios no relacionados con las funciones del rol y actividades de la Corporación.

2.11.7 RESPECTO A REPORTAR INCIDENTES

2.11.7.1 El cumplimiento y observación de esta política tiene como objetivo principal la protección de nuestra información y activos. En caso de incidentes el usuario tiene la responsabilidad de notificar inmediatamente a su supervisor inmediato y al equipo de tecnología a través de la mesa de servicios de TI. Algunos de los incidentes más comunes, pero no limitados a esta lista, son:

I. Robo o pérdida de equipo, tanto el proporcionado por la compañía como el propio conteniendo información de TechCore.

II. Sospecha de uso de credenciales por parte de alguna otra persona.

III. Comportamiento inconsistente con la política por parte de compañeros de trabajo.

IV. Mensajes o llamadas telefónicas solicitando información personal o sus credenciales de acceso.

V. Mensajes de correo electrónico solicitando información personal o credenciales de acceso.

VI. Uso para fines personales de las instalaciones, infraestructura, equipo y/o material que TechCore ha puesto a disposición para nuestras actividades laborales.

2.12 CONTINUIDAD DE TI

2.12.1 ANÁLISIS DE IMPACTO

2.12.1.1 Se debe identificar los procesos críticos, sus riesgos asociados y el impacto que estos puedan tener sobre el negocio con el objetivo de identificar los controles y acciones correspondientes para procurar la recuperación efectiva de las actividades laborales, evitando o reduciendo al mínimo el daño a colaboradores, rentabilidad, reputación o capacidad de operación.

2.12.2 **PLAN DE CONTINUIDAD DE TI**

2.12.2.1 Se deben diseñar y elaborar planes de continuidad de TI para apoyar en la continuidad de los procesos más críticos de la corporación. Lo anterior con el objetivo de garantizar la continuidad de las operaciones críticas en caso de situaciones de emergencia que produzcan paralización parcial o total de la capacidad operativa. Para tal efecto, se deberán establecer las pautas a seguir para su desarrollo, actualización, prueba y puesta en marcha.

2.12.2.2 El Plan de Continuidad de TI tiene por objetivo principal la recuperación de los sistemas críticos en márgenes de tiempo y niveles de servicios acordes a las necesidades de las distintas unidades de negocio.

2.12.3 **PRUEBAS Y SEGUIMIENTO DEL CUMPLIMIENTO DE LOS PLANES DE CONTINUIDAD**

2.12.3.1 Se deben realizar pruebas periódicas sobre el cumplimiento de los Planes de Continuidad establecidos.

2.12.4 **OBLIGACIONES LEGALES Y CONTRACTUALES**

2.12.4.1 Con base en los requerimientos contractuales, se deben preparar, mantener y probar regularmente planes para asegurar la continuidad del negocio. Garantizando el cumplimiento de las obligaciones contraídas con terceros, mediante la aplicación y revisión por lo menos una vez al año, dejando evidencia en el registro correspondiente con el fin de prevenir impactos adversos en la prestación del servicio.

2.13 GESTIÓN DE RIESGO DE TI Y SEGURIDAD DE LA INFORMACIÓN

2.13.1 Se debe contar con una metodología, que permita la identificación de los activos de información con mayor impacto en el cumplimiento de los objetivos de TechCore, los riesgos de tecnología y de seguridad de la información a los que estos se encuentran expuestos y las estrategias a seguir para su gestión.

2.13.2 Se debe contar con un Programa de Administración del Riesgo de Seguridad de forma periódica que permitirá identificar las vulnerabilidades y amenazas a las que están expuestos los activos críticos de información, revaluar el riesgo en términos de su impacto y probabilidad de ocurrencia, establecer las acciones necesarias para su mitigación, y generar modificaciones al modelo de seguridad acordes con las nuevas necesidades de protección de la Organización.

2.14 GESTIÓN DE INCIDENTES

2.14.1 Todo incidente de seguridad debe ser tratado desde su detección hasta su resolución, mediante un procedimiento establecido para el adecuado tratamiento de incidentes.

2.14.2 Se debe contar con una herramienta que apoye el proceso de atención, seguimiento y cierre de los incidentes de seguridad, que en la medida de lo posible pueda emitir métricas de eficiencia en la resolución de los incidentes, permita asignar prioridades y llevar un registro del estado de las actividades de investigación para la resolución. En todo caso, los incidentes de seguridad no deben ser cerrados hasta que estén totalmente resueltos y documentados, debe incluirse en la documentación del caso, las recomendaciones que surjan como resultado del procedimiento que se haya utilizado para su resolución.

2.14.3 Los incidentes y problemas de seguridad deben ser manejados por el personal interno de la Unidad de Seguridad de Información y Continuidad de Negocio.

2.14.4 Debe definirse los canales de comunicación oficiales para el reporte de incidentes de ciberseguridad y seguridad de la información.

2.14.5 Todo el personal que administra la infraestructura tecnológica debe estar capacitado para la gestión de incidentes de seguridad de la información.

2.14.6 DOCUMENTAR PLAN DE GESTIÓN DE CRISIS

Identificar un equipo primario de gestión de crisis que coordinará la evaluación de los eventos, incidentes, crisis y desastres para determinar la forma en la cual la Organización responderá al suceso según el Plan Gestión de Crisis.

2.15 SANCIONES

2.15.1 El incumplimiento de esta política incluirá sanciones administrativas que pueden variar de acuerdo con la severidad desde una llamada de atención verbal con anotación al expediente hasta la desvinculación de la compañía.

2.15.2 Cuando la falta lo amerite, la misma deberá ser reportada al Comité de Ética del país correspondiente, siendo el comité del país respectivo quien recomiende la sanción a aplicar en caso de fallas a la política y en los casos de alto impacto, deberá ser escalado al Comité Central de Ética.

2.15.3 El comité de ética de cada país será quien recomiende la sanción a aplicar en caso de fallas a la política y en el caso de escalaciones al Comité Central de Ética.