ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR

POLITICA DE SEGURIDAD DE LA INFORMACION

GERENCIA Y DIRECCIONAMIENTO

Elaboró	Utima Actualización Realizada Por:	Ultima Revisión Realizada Por:	Aprobó
Fabian Pinedo Villafañe Director Sistemas	Fabian Pinedo Villafañe Director Sistemas	Alexander Salcedo G. Director Gestion Humana	Comité de dirección ACTA 55 11 de abril del 2025

1. INTRODUCCIÓN

La organización Clínica Bonnadona Prevenir, en adelante OCBP, determina la información como un activo de alta importancia para la entidad, indispensable para alcanzar los objetivos estratégicos de la organización. Por consiguiente, es necesario disponer de estrategias, lineamientos y reglas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

2. OBJETIVO

El objetivo principal de esta política es establecer los principios y lineamientos necesarios para proteger, conservar y asegurar los recursos de información de la organización, garantizando su confidencialidad, integridad y disponibilidad.

2.1. OBJETIVO ESPECÍFICO

- Implementar medidas de seguridad que reduzcan riesgos de amenazas a la información.
- Restringir el acceso a los datos únicamente a personas autorizadas.
- Regular la adquisición de software, desarrollo de aplicaciones y uso de aplicaciones externas.
- Establecer estrategias de continuidad frente a incidentes de seguridad.
- Proteger los activos de información durante todo su ciclo de vida.

- Garantizar una transmisión de información segura y sin alteraciones indebidas.
- Fomentar una cultura de seguridad de la información en empleados, contratistas, proveedores y clientes.

3. **ALCANCE**

Esta política aplica a:

- Todo el personal de la Organización Clínica Bonnadona Prevenir (OCBP), independientemente de su tipo de contratación.
- Personal externo como consultores, asesores, auditores o terceros con vínculo contractual o no remunerado.
- Todos los activos de información actuales o futuros de la organización, sin importar su soporte (impresos, electrónicos, audiovisuales o verbales).
- Todos los procesos de negocio, bajo un enfoque de mejoramiento continuo y de cumplimiento obligatorio, incluyendo sanciones por incumplimiento.

4. **DEFINICIONES**

- Acceso remoto: conexión a recursos ubicados en equipos de otra localización mediante red local o externa.
- Activo: cualquier recurso con valor para la organización que requiera protección (información, sistemas, equipos, servicios).
- Amenaza: causa potencial de un incidente no deseado que puede afectar a la organización.
- Análisis de riesgos: proceso sistemático para identificar y estimar riesgos de seguridad de la información.
- Autenticación: proceso para validar la identidad de un usuario o sistema.
- Confidencialidad: acceso a la información únicamente por personal autorizado.
- Disponibilidad: garantizar acceso a la información y sistemas cuando se requiera.
- Integridad: asegurar la exactitud y completitud de la información y sus procesos.
- Inventario de activos: listado de todos los recursos dentro del alcance del SGSI que requieren protección.
- VPN: red privada virtual que permite conexiones seguras sobre redes públicas mediante cifrado.
- WiFi: tecnología de interconexión inalámbrica de dispositivos electrónicos.

5. **NORMATIVIDAD APLICABLE**

- NTC-ISOIIEC 27001- 27002:2022: norma internacional para los sistemas de gestión de la seguridad de la información. (SGSI)
- Ley 1273 de 2009: Ley de protección de la información y de los datos
- Ley 1581 de 2012: Ley de protección de datos personales
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1266 de 2008: también conocida como Ley de Habeas Data, se aplica a todos los datos personales financieros, crediticios, comerciales y de servicios registrados en un banco de datos.

6. **RESPONSABILIDAD**

- ALTA DIRECCIÓN
- Promueve funciones y responsabilidades en seguridad de la información.
- Facilita recursos adecuados para alcanzar los objetivos de seguridad.
- Impulsa la divulgación y concienciación de la Política de Seguridad.
- Exige el cumplimiento de la Política, la legislación vigente y requisitos regulatorios.
- Considera los riesgos de seguridad de la información en la toma de decisiones.

- **DIRECCIÓN DE SISTEMAS**
- Revisa y propone la Política de Seguridad de la Información a la alta dirección para su aprobación.
- Estructura, recomienda, da seguimiento y mejora el SGSI.
- Lidera estas funciones con apoyo del jefe de sistemas, coordinadores y asesor de seguridad informática.

- **GRUPO RESPONSABLE DE SEGURIDAD INFORMÁTICA**
- Supervisa el cumplimiento de la Política en temas operativos y técnicos.
- Administra y monitorea plataformas de seguridad.
- Está conformado por el jefe de sistemas, coordinadores y un técnico especializado.

- **PROPIETARIOS DE ACTIVOS DE INFORMACIÓN**
- Mantienen la confidencialidad, integridad y disponibilidad de los activos bajo su responsabilidad durante todo su ciclo de vida.

- **RECURSOS HUMANOS**
- Notifica a todo el personal sobre sus obligaciones en seguridad de la información al iniciar la vinculación.
- Gestiona la firma de compromisos o cláusulas de confidencialidad.
- Organiza capacitaciones continuas en seguridad, conforme a esta Política.

- **JURÍDICA**
- Verifica que los contratos y acuerdos cumplan con la Política de Seguridad.
- Asesora legalmente a la organización en temas de seguridad de la información.

- **USUARIOS DE LA INFORMACIÓN**
- Deben conocer y cumplir la Política de Seguridad vigente.
- Son responsables del uso adecuado de los sistemas y de proteger la información a la que acceden.

- **EMPLEADOS, TERCEROS Y CONTRATISTAS**
- Cumplen lo establecido en la Política en su entorno laboral.
- Están obligados a reportar de manera oportuna cualquier incidente de seguridad detectado.

7. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**

La OCBP establece un marco de referencia para la gestión de la seguridad de la información, garantizando su implementación, control y mejora continua.

- Compromiso de la Alta Dirección: Brinda apoyo, liderazgo y asigna presupuesto para actividades de seguridad y gestión de riesgos.
- Gestión de riesgos y políticas: Se define un espacio formal para el análisis de riesgos, revisión de políticas y tratamiento de problemas de seguridad de la información.
- Roles y responsabilidades: Las funciones relacionadas con seguridad deben estar claramente definidas, documentadas y asignadas a personal capacitado.
- Relaciones con autoridades: Se mantienen contactos con organismos reguladores y autoridades pertinentes para consultas, emergencias e incidentes.
- Participación en foros especializados: El personal de seguridad mantiene contacto con grupos de interés y comunidades profesionales de seguridad.
- Gestión de proyectos: Todo proyecto institucional debe incluir un análisis de riesgos de la información en su planeación y ejecución.

8. **POLITICA DE SEGURIDAD DEL RECURSO HUMANO**

La organización establecerá mecanismos para garantizar que empleados y contratistas comprendan sus responsabilidades en seguridad de la información y sean idóneos para sus funciones.

8.1**. ANTES DE LA CONTRATACIÓN**

- El área de Gestión Humana deberá contar con un procedimiento documentado de selección de personal.
- Dicho procedimiento incluirá verificación de referencias y antecedentes conforme a la ley y normativa vigente.
- Si la validación se realiza mediante un proveedor externo, este deberá cumplir con los requisitos de la política de seguridad.
- Para cargos con roles críticos en el manejo de información, se aplicarán procesos de selección reforzados.

8.2. DURANTE LA EJECUCIÓN DEL CONTRATO

- Todos los empleados y contratistas deberán cumplir las políticas y procedimientos de seguridad de la información.
- La organización implementará un programa de cultura y capacitación en seguridad dirigido a todos los niveles, incluida la alta gerencia.
- El programa se basará en riesgos clave y responsabilidades de cada rol, incluyendo actividades de sensibilización, pruebas periódicas y acciones de mejora.
- El contenido deberá actualizarse considerando nuevas amenazas, vulnerabilidades, incidentes y cambios en las políticas.
- El personal con funciones críticas de seguridad deberá contar con las competencias técnicas necesarias y capacitación continua.
- Se establecerán canales de comunicación formales (intranet, correos, carteles, capacitaciones virtuales, boletines) para difundir información de seguridad.

8.3. TERMINACIÓN O CAMBIO DE EMPLEO

- Las obligaciones de seguridad que persistan tras la terminación o cambio de contrato deberán ser comunicadas y exigibles.
- En casos de retiro o traslado de cargo, se revisarán y ajustarán los accesos de usuario, asegurando la confidencialidad de la información.
- El área de Sistemas y Gestión Humana deberán garantizar la devolución de activos de información, credenciales y equipos asignados.

9. **POLITICA DE GESTION DE LOS ACTIVOS DE INFORMACIÓN**

Esta política busca la preservación de los activos de información como soporte del negocio.

9.1. RESPONSABILIDAD Y USO DE LOS ACTIVOS DE INFORMACIÓN

Los usuarios, proveedores y terceros que utilicen activos de información deberán:

- Usar la información y sistemas solo para fines autorizados y laborales.
- Proteger los activos físicos y lógicos bajo su custodia.
- No compartir contraseñas ni accesos sin autorización.
- Devolver los activos al finalizar su contrato o relación laboral.
- Mantener la confidencialidad de toda la información institucional.

La organización establece reglas para el uso adecuado de sus activos tecnológicos, información y sistemas de procesamiento.

9.1.1 SISTEMA OPERATIVO

- Solo se permite el uso de sistemas operativos autorizados y configurados por el área de Sistemas.
- El acceso a configuraciones administrativas está limitado al personal de Sistemas.
- Los usuarios no podrán instalar, modificar ni actualizar el sistema operativo sin autorización.
- Los equipos deberán contar con bloqueo automático tras inactividad.

9.1.2 INTERNET

- El acceso a Internet es una herramienta laboral y será monitoreado por TI.
- Se prohíbe acceder a sitios no relacionados con funciones institucionales.
- Solo personal autorizado podrá descargar información o software, sujeto a revisión de seguridad.
- Todo tráfico será registrado y sujeto a auditoría; los accesos indebidos se reportarán a la Gerencia.

9.1.3 CORREO ELECTRÓNICO

- El correo institucional es de uso exclusivo laboral y para personal autorizado.
- Está prohibido el envío de cadenas, spam, alertas no autorizadas o contenido ofensivo.
- No se permite suplantar identidades ni interceptar comunicaciones.
- Los correos sospechosos deberán reportarse de inmediato al área de Sistemas.
- Está prohibido que los usuarios envíen alertas de seguridad. Si algún usuario recibe una alerta de seguridad debe reenviarla al departamento de sistemas, específicamente al correo ciberseguridad@bonnadona.co

9.2. CLASIFICACION DE LA INFORMACION

- La información será clasificada según su valor, criticidad y requisitos legales en niveles: pública, uso interno, confidencial y crítica.
- Cada nivel tendrá controles de seguridad definidos (etiquetado, protección de acceso, cifrado).
- Se aplicarán procedimientos para el manejo seguro de activos según su clasificación.

9.3. POLITICA DE MANEJO DE MEDIOS

Los medios removibles (USB, discos externos, CD/DVD, cintas, etc.) deberán gestionarse bajo controles de seguridad que garanticen la protección de la información.

- Los medios deberán almacenarse, transportarse y desecharse de manera segura.
- Toda información obsoleta deberá eliminarse con borrado seguro o destrucción física.
- Se mantendrá un registro actualizado de todos los medios asignados.

9.3.1. GESTION DE MEDIOS REMOVIBLES

- El área de Sistemas autorizará y controlará el uso de medios removibles.
- Los usuarios son responsables de custodiar la información contenida en los medios asignados.
- Los medios removibles no podrán usarse como alternativa de respaldo, salvo autorización formal.
- Los dispositivos deberán analizarse con antivirus antes de su uso.
- La pérdida de medios removibles deberá notificarse de inmediato como incidente de seguridad.

9.3.2. GESTIÓN DE LA TRANSFERENCIA DE INFORMACION

- La información no podrá transferirse a terceros sin autorización formal y compromiso de confidencialidad.
- Toda transferencia deberá realizarse bajo mecanismos seguros (cifrado, mensajería certificada).
- El transporte físico de medios debe garantizar protección contra accesos no autorizados.
- Se deberá dejar constancia de recepción en cada proceso de transferencia.

10. POLITICA DE CONTROL DE ACCESO

La organización debe definir lineamientos y mecanismos para limitar el acceso a la información y a instalaciones de procesamiento de información.

10.1. SEGURIDAD FÍSICA Y DEL ENTORNO

- El acceso físico a áreas críticas (datacenter, salas de servidores, cuartos de telecomunicaciones) estará restringido mediante controles biométricos, tarjetas electrónicas y videovigilancia.
- Todo ingreso deberá registrarse en bitácoras físicas o electrónicas, indicando persona, fecha, hora y motivo.

- Los visitantes deberán estar acompañados en todo momento por personal autorizado.

10.2. GESTIÓN DE ACCESO A USUARIOS

- Cada usuario contará con credenciales únicas; se prohíbe el uso de cuentas compartidas o genéricas.
- Se aplicará autenticación multifactor (MFA) en todos los sistemas críticos.
- Los privilegios de acceso se otorgarán bajo el principio de mínimo privilegio y se revisarán semestralmente.
- Al finalizar la relación laboral o contractual, los accesos deberán revocarse de forma inmediata.

10.3. ACCESO A REDES Y SERVICIOS DE RED

- El acceso remoto deberá realizarse únicamente mediante VPN corporativa con cifrado TLS 1.2 o superior y en lo posible MFA.
- La red corporativa será segmentada (ejemplo: administrativa, clínica, invitados), y el tráfico entre segmentos deberá ser controlado mediante firewalls y reglas de seguridad.
- Los servicios de red (DNS, DHCP, correo, proxy) deberán estar protegidos con mecanismos de endurecimiento y monitoreo en tiempo real.

10.4. ACCESO A SISTEMAS Y APLICACIONES

- Todo acceso a sistemas y aplicaciones críticas deberá registrarse y auditarse periódicamente.
- Las cuentas con privilegios administrativos deberán ser controladas mediante soluciones de gestión de accesos privilegiados (PAM) o mecanismos equivalentes.
- Los sistemas deberán implementar controles de sesiones (tiempo de inactividad máximo, cierre automático, bloqueo tras intentos fallidos).

10.5. TRABAJO EN ÁREAS SEGURAS

- El acceso a áreas seguras estará limitado exclusivamente a personal autorizado.
- Los visitantes externos deberán estar acompañados y usar credenciales temporales.
- Se prohíbe el ingreso de dispositivos no autorizados (USB, discos externos, teléfonos móviles sin aprobación).

10.6. PROVEEDORES ESPECIALES

- Los proveedores de servicios especializados (biomédico, redes, servidores, telecomunicaciones) estarán sujetos a controles de acceso más rigurosos.
- Sus accesos serán temporales, justificados y supervisados en todo momento.
- Deberán firmar acuerdos de confidencialidad y cumplir con las políticas de seguridad institucional.
- Todo acceso será registrado y auditado posteriormente.

11. GESTIÓN DE RELACIONES CON PARTES INTERESADAS

La Organización Clínica Bonnadona Prevenir (OCBP) establece mecanismos para garantizar que las relaciones con partes interesadas internas y externas no comprometan la confidencialidad, integridad y disponibilidad (CID) de la información.

MEDIDAS DE CONTROL:

- Identificación y evaluación de partes interesadas según el impacto en la seguridad de la información.
- Inclusión de cláusulas contractuales sobre confidencialidad y cumplimiento normativo.
- Evaluación periódica de proveedores y terceros respecto a requisitos de seguridad.
- Definición de políticas de acceso a sistemas y activos bajo principios de mínimo privilegio y necesidad de conocer.
- Comunicación formal y oportuna ante incidentes de seguridad que puedan afectar servicios o información compartida.

11.1. RELACIONES CON PROVEEDORES

La OCBP establece lineamientos de seguridad con proveedores y terceros que tengan acceso a activos o sistemas de información.

ACUERDOS CON PROVEEDORES:
Los contratos deben contemplar requisitos de seguridad antes, durante y después de la relación contractual, incluyendo:

- Descripción de la información y su método de acceso.
- Clasificación de la información involucrada.
- Notificación inmediata de incidentes de seguridad.
- Condiciones sobre subcontratación y restricciones en relaciones con terceros.
- Responsabilidades en gestión de riesgos y seguridad.
- Control del personal vinculado al servicio.
- Cumplimiento de requisitos legales y normativos.
- Uso adecuado de los activos de información.
- Derecho de monitoreo y auditoría por parte de OCBP.
- Identificación de controles físicos y lógicos aplicados.
- Información actualizada de contacto del proveedor.

ADQUISICIONES:

- El área de Sistemas define requisitos de seguridad para toda adquisición de hardware y software, de acuerdo con el procedimiento de compras.
- Los proveedores de TIC deben garantizar que las medidas de seguridad de OCBP se extiendan a sus propios terceros involucrados.

SEGUIMIENTO A PROVEEDORES:

- Se realizarán seguimientos periódicos, considerando tipo de proveedor, acuerdos de nivel de servicio (SLA) y criticidad de la información manejada.
- Se podrán ejecutar auditorías de tercera parte cuando lo exija la ley o lo considere OCBP.
- Los contratos deben incluir cláusula de terminación por incumplimiento de políticas de seguridad.
- Los supervisores de contratos de OCBP deben monitorear los servicios prestados, realizar revisiones periódicas y aplicar recomendaciones derivadas de auditorías.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información reportados en la organización al correo **ciberseguridad@bonnadoda.co**. Estos deben gestionarse adecuadamente. De tal manera que exista un marco para la identificación, clasificación, respuesta y análisis de incidentes de seguridad de la información, garantizando la continuidad del negocio, la protección de la información y la mejora continua de los controles de seguridad.

13. CUMPLIMIENTO

La OCBP establece mecanismos para garantizar el cumplimiento de esta política, así como de los requisitos legales y contractuales en materia de seguridad de la información. El incumplimiento puede conllevar sanciones disciplinarias según la gravedad.

13.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

- Identificación, documentación y actualización de normas legales, reglamentarias y contractuales aplicables.
- Protección de registros contra pérdida, destrucción, falsificación o acceso no autorizado.
- Cumplimiento de normativas sobre privacidad, protección de datos personales y propiedad intelectual.
- Uso de controles criptográficos cuando corresponda.
- Uso legal de software, con comunicación de políticas y consecuencias en caso de incumplimiento.

13.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

- Revisión periódica de la gestión de seguridad y su cumplimiento por líderes de área y auditorías técnicas.
- Evaluación regular de sistemas y aplicaciones para verificar cumplimiento normativo.
- Identificación y corrección de vulnerabilidades técnicas bajo un enfoque basado en riesgos.

13.3. VIGENCIA DE LA POLÍTICA

La política entra en vigor al ser oficializada y comunicada. Todo nuevo personal debe firmar aceptación. Cualquier conflicto con regulaciones debe reportarse de inmediato.

13.4. GESTIÓN DE EXCEPCIONES

Las excepciones deben registrarse y analizarse por el área de Sistemas, con aprobación de la Gerencia según el nivel de riesgo.

13.5. SANCIONES DISCIPLINARIAS

El incumplimiento será sancionado conforme a los procesos internos. Todo colaborador debe reportar incidentes o violaciones a la política.

13.6. AUDITORÍAS

Se realizan auditorías internas y externas periódicas para:

- Verificar cumplimiento de políticas y controles.
- Identificar no conformidades y oportunidades de mejora.
- Asegurar la mejora continua del SGSI.
- Los hallazgos se documentan, informan a la alta dirección y generan planes de acción con seguimiento y cierre en plazos definidos.