POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.1

Elaborado por:	Revisado y aprobado por:	Actualizado por:
Ing. Reynaldo Gaibor MSc. Fecha: 03-2022	Gerencia General – GG Fecha: 05-2023	Proyectos TI – EA / 05-2023

Contenido

1 CONTROL DEL DOCUMENTO

DATOS GENERALES DEL DOCUMENTO VIGENTE			
Código PMO	**Versión**	**Nombre**	**Autor**
PC-PSI-1	1.1	Actualización de funciones, distribución y localización	Ti. Edison Acosta

FIRMA DE APROBACIÓN		
	DRA. CARMEN ELENA CEPEDA	GERENTE GENERAL

LISTADO DE DISTRIBUCIÓN		
GLOBAL SUPPORT	DRA. CARMEN ELENA CEPEDA	GERENTE GENERAL
GLOBAL SUPPORT	PAOLA CORO	JEFE DE PRODUCCIÓN
GLOBAL SUPPORT	ING. CRISTINA CEPEDA	ENCARGADA DE SEGURIDAD
GLOBAL SUPPORT	ING. MANUEL SOSA M.	ADMINISTRADOR DEL EDIFICIO
GLOBAL SUPPORT	GINA BAQUE	BRIGADA DE P. AUX
GLOBAL SUPPORT	PATRICIO VÁSQUEZ	BRIGADA DE P. AUX
GLOBAL SUPPORT	EC. EDISON CEPEDA	GERENTE FINANCIERO
GLOBAL SUPPORT	DR. EDUARDO HERMOSA	GERENTE LEGAL

REGISTROS DE CAMBIOS EN EL DOCUMENTO			
Versión	**Descripción del cambio**	**Realizado por**	**Fecha**
1.0	Documento Original	Ing. Reynaldo Gaibor MSc.	03/2022
1.1	Actualización de funciones, distribución y localización	TI. Edison Acosta	05/2023

2. INTRODUCCIÓN

Global Support S.A es una empresa con presencia a nivel nacional que brinda respaldo y seguridad a todos sus clientes mediante la prestación de servicios de asesoría empresarial, y está calificada para brindar servicios auxiliares de cobranza a entidades financieras y del sistema cooperativo, con un equipo humano y profesional con alta experiencia, comprometido con la búsqueda de resultados.

Este documento presenta una versión actualizada de las Políticas de Seguridad de la Información para Global Support.

Con la publicación de este documento, se pretende que los empleados y terceros externos a la empresa, que tenga relación directa con Global Support, conozcan y den cumplimiento al marco normativo de las Políticas de Seguridad de la Información.

La gestión de la seguridad de la información en Global Support, se basa en estándares internacionales para la evaluación de riesgos que pudieren vulnerar la confidencialidad, integridad o disponibilidad de los activos de información, por lo que el presente documento debe ser revisado a intervalos planificados, o si ocurriesen cambios significativos en los procesos principales de la institución; esto con el fin de asegurar que se mantenga la idoneidad, adecuación y eficacia del mismo.

3. OBJETIVO DEL DOCUMENTO

Establecer un marco de referencia basado en el cuerpo de normas internacionales ISO 27000, para la generación e implementación de normas y procedimientos referidos a derechos, obligaciones y responsabilidades aplicables a los empleados de Global Support respecto de los activos de información a los cuales tienen acceso y así lograr niveles adecuados de integridad, confidencialidad y disponibilidad para los activos de información críticos de la empresa.

Físico: Guía orientada al personal autorizado para tomar medidas efectivas en caso de un posible incidente en las áreas tangibles de la empresa, especificadas en distintos casos que pueden afectar el bienestar y continuidad del negocio.

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.1 ROLES Y RESPONSABILIDADES

a. La Gerencia General de Global Support debe garantizar que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información.

b. La Gerencia General debe designar al responsable de administrar el programa de seguridad de la información, con las atribuciones:

- Elaboración de políticas en materia de Seguridad de la Información para conocimiento, revisión y aprobación de la Gerencia General.
- Preparar el plan de formación y sensibilización para la seguridad de la información.
- Revisar las normativas, procesos y/o procedimientos que sean elaborados por las diferentes áreas que involucren a la seguridad de la información y velar por el cumplimiento de estas.
- Apoyar en la elaboración de propuestas en planes de contingencia para la continuidad y recuperación de desastres en materia de seguridad de la información, en conjunto con las áreas pertinentes.

c. Todas las direcciones y departamentos de Global Support deben alinear sus procesos de gestión y operación a las Políticas de Seguridad de la Información y brindar el apoyo al responsable de administrar el programa de seguridad de la información.

d. Para la aplicación de la Ley Orgánica de Protección de Datos Personales se conforma un comité constituido por:

- Gerente General.
- Gerente Administrativo Financiero.

- Gerente Jurídico.
- Responsable de Seguridad de La Información.

4.2 RECURSOS HUMANOS

a. La selección del personal es responsabilidad de la Gerencia Administrativa Financiera, quien realiza la evaluación integral del personal, asegurando que el perfil de competencias del candidato es el más adecuado para cumplir con el puesto requerido, además de corroborar los antecedentes y/o referencias laborales del mismo.

b. Los empleados deben:

- Cumplir las políticas, normativas, lineamientos y/o reglamentos definidos por la empresa.
- Utilizar las herramientas tecnológicas institucionales para el cumplimiento de sus labores.
- Cumplir con los procedimientos establecidos por la empresa.
- Cumplir con los planes y programas que promuevan la seguridad de la información de la empresa.

c. La Gerencia Administrativa Financiera en conjunto con el área requirente deben definir responsabilidades para los contratistas o terceros según el servicio o bien que requiera la empresa y la normativa pertinente vigente.

d. Todos los proveedores, contratistas o terceros que tengan acceso a los activos de información de la deben firmar el Acuerdo de Confidencialidad establecido.

4.3 GESTIÓN DE ACTIVOS

a. La Gerencia General coordinará con las áreas pertinentes de la empresa la identificación de sus activos de información, su clasificación y las responsabilidades de protección apropiadas.

b. Todo activo de información debe ser asignado a un responsable quien debe:

- Salvaguardar la integridad, disponibilidad y confidencialidad del activo.

- Hacer uso del activo únicamente para los propósitos y actividades de la empresa, sometiéndose a las consecuencias de incurrir en faltas estipuladas en leyes y reglamentos.
- Reportar cualquier incidente o problema relacionado con el activo de información. Cualquier omisión (con dolo o involuntaria) de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información.
- Realizar lo necesario para mantener el activo de información en buenas condiciones que garantice y cumplan su función.
- Definir la retención y eliminación de datos, en los casos que amerite.

c. Los custodios de activos deberán mantener un nivel adecuado de protección sobre la modificación o destrucción no autorizada.

d. Todo medio extraíble que pertenezca a la institución debe ser asignado a un custodio y éste será el responsable de proteger la información almacenada en el mismo.

e. Cualquier información cuya divulgación, publicidad, comunicación o conocimiento pueda afectar los derechos, el cumplimiento de los objetivos legales de la empresa, será considerada información de alta criticidad.

4.4 SEGURIDAD FÍSICA

a. La Gerencia Administrativa Financiera emitirá las directrices para evitar el acceso físico no autorizado, daño e intromisiones a la información e instalaciones de procesamiento y transmisión de la información.

b. El edificio Sense consta con sensores de ingreso, circuito de televisión cerrado, accesos magnéticos a elevadores y registro de visitantes con bitácoras.

c. La recepción de Global Support debe mantener una bitácora de los visitantes a la empresa con al menos el siguiente detalle:

- Fecha y hora de ingreso.

- Hora de salida.
- Nombres y apellidos del visitante y empresa a la que pertenece.
- Número de cédula y/o documento de identificación.
- Dependencia / empresa.

- Actividad y empleado que lo recibirá
- Firma de aprobación.

d. Se debe aplicar la normativa y procedimientos establecidos en los planes de contingencia y plan de recuperación de desastres, de acuerdo con la ubicación de los centros de datos y cuartos de comunicación.

e. Se debe definir planes y rutas de evacuación con señalética para todo inmueble donde opere la empresa y socializar a todos los empleados.

f. Todos los trabajos técnicos ejecutados por externos a la empresa deben ser supervisados.

g. El rack de comunicaciones de Global Support debe permanecer cerrado bajo llave que será custodiada por el responsable de sistemas, y mantendrá bitácora de las actividades que requieran el acceso al mismo.

h. Se prohíbe la copia o transferencia de la información de la empresa sin previa autorización al momento de ejecutar los trabajos.

i. Se prohíbe filmar, tomar fotos y grabar videos en las oficinas de la empresa, excepto al personal autorizado por la Gerencia General.

j. No se permite el ingreso de personas en estado de embriaguez o bajo el efecto de sustancias psicotrópicas o alucinógenas a las oficinas de la empresa.

k. La sesión de usuario en una estación de trabajo se debe bloquear una vez alcanzado el periodo de inactividad predefinida. El desbloqueo de la estación de trabajo o terminal debe ser por medio de contraseñas o mecanismos biométricos.

l. Los empleados que dejen desatendida su estación de trabajo asignado deben bloquearlo de forma obligatoria.

m. Los documentos con información crítica o confidencial no deben permanecer desatendidos o expuestos en el área de trabajo.

n. Todo empleado debe retirar de manera inmediata la documentación de impresoras / fotocopiadoras.

o. Todo empleado es responsable de la documentación que imprima.

4.5 SEGURIDAD EN LAS OPERACIONES

a. Proteger la información y las instalaciones de procesamiento de la información contra ataques informáticos como: malware, phishing, robo de datos y propiedad intelectual, entre otros ya sean internos o externos.
b. Almacenar, mantener y revisar periódicamente eventos que registran las actividades de los usuarios, las excepciones, los fallos y los eventos de seguridad de la información y mantenerlos como evidencia.
c. El responsable de sistemas es responsable del diseño, implementación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones de la empresa.

4.6 CONTROL DE ACCESO

a. Deben establecerse controles para el acceso a la información y a los recursos de procesamiento de la información.
b. Los controles de acceso a la información deben asignarse con base en roles y perfiles de usuarios.
c. Debe comunicarse al encargado de la creación de usuarios sobre los empleados que son vinculados / desvinculados de la empresa.
d. Es responsabilidad de todos los empleados de Global Support, salvaguardar la confidencialidad y buen uso de las credenciales digitales asignadas para acceso a los sistemas informáticos de la empresa.
e. Corresponde al responsable de sistemas elaborar la política de contraseñas para Global Support.

4.7 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO

a. El responsable de sistemas debe establecer controles en la infraestructura tecnológica para evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones informáticas de la empresa.

b. El responsable de sistemas debe llevar un inventario de los sistemas, sus dependencias y componentes, así como también debe depurar los recursos que no se están utilizando en la empresa.
c. La instalación y configuración de los sistemas en ambientes productivos y no productivos debe ser ejecutada en el ámbito de sus competencias por el responsable de sistemas según sus atribuciones.
d. La actualización del sistema operativo, aplicaciones y programas en ambientes productivos debe realizarse de acuerdo con el proceso de control de cambios.
e. Los servidores de producción deben contener únicamente aplicaciones, códigos, y programas aprobados para funcionar en ese ambiente, según el procedimiento de paso a producción.
f. La restauración de las bases de datos de producción en ambientes no productivos debe enmascarar los datos sensibles, a excepción de la información que se requiera para la resolución de incidentes y capacitación.
g. El proceso de restauración y enmascaramiento de la información de las bases de datos de ambientes no productivos estará a cargo del responsable de sistemas.
h. Las especificaciones técnicas para la adquisición de software o para su desarrollo externo, deben incluir un procedimiento de recepción, en el cual se detalle las etapas de desarrollo, pruebas (calidad y seguridad) y aceptación funcional.
i. Debe publicarse en la página web de la empresa para conocimiento de sus visitantes, el aviso de la política de privacidad.

4.8 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a. Global Support mantendrá vigente un contrato de servicio de SOC (Security Operation Center) de gestión de ciberseguridad con alerta temprana de eventos y/o incidentes de nivel crítico que pudiese ser un indicador de compromiso de seguridad para la red de la empresa, con una disponibilidad del servicio (SLA) de al menos 99,6%.

b. Cuando el SOC identifique un evento de ciberseguridad sobre Global Support, procederá a la notificación vía correo electrónico con información relevante como:
   - IP del host que está comprometido
   - El tipo de anomalía detectado
   - Información completa de las conexiones realizadas (IP origen, IP destino, URL, dominio, categoría, acción tomada, entre otros)
   - Resumen del posible impacto o daño que pudiese causar, por ejemplo, robo de información personal (contraseñas, tarjetas de créditos, entre otros).
   - La posible causa de la infección.
   - Las recomendaciones que el equipo de ciberseguridad del SOC recomienda ejecutar para solventar la problemática detectada.

c. El monitoreo del SOC debe detectar los eventos de seguridad basados en al menos los casos de uso que se mencionan a continuación:
   - IOC (Indicadores de compromiso).
   - Botnets.
   - Escaneo de puertos.

d. Global Support deberá comunicar al SOC los contactos y vías de comunicación necesarios mediante los cuales recibirá las notificaciones de los eventos detectados para la gestión oportuna de los mismos.

4.9 CUMPLIMIENTO

a. Global Support debe implementar procedimientos que garanticen el cumplimiento de los requisitos legales, normativos y contractuales relacionados con los derechos de propiedad intelectual y el uso de software propietario.

b. La empresa debe determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

c. Debe almacenarse los registros y evitar pérdidas, destrucción, falsificación, accesos y publicación no autorizados

d. Los ejecutivos que ejercen cargos directivos de Global Support deben revisar periódicamente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
e. Debe implementarse controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
f. Debe revisarse y actualizarse este documento al menos una vez al año.

5. DOCUMENTOS DE REFERENCIA

Documento	Código	Descripción	Tipo de Documento
Procedimiento De Respaldos	PRO- PR-1	Manual y procedimiento para la generación y tratamientos de respaldos	Físico y Digital
Procedimiento Para Administración De Servidores	PC- PAS	Manual y procedimiento para el cuidado y los parámetros correcto en la configuración de los servidores.	Físico y Digital
Procedimiento Gestión De Monitoreo, Eventos E Incidente	PC- GMEI	Manual y procedimiento para la obtención y manejo de los incidentes.	Físico y Digital
Procedimiento Control De Accesos	PC- CAC	Manual y procedimiento para la creación privilegios y desvinculación de los usuarios	Físico y Digital
Retención Y Eliminación De Información Sensible	PC- PGQS	Manual y procedimiento para el tratamiento de la información sensible,	Físico y Digital
Procedimiento Para Gestión De Parches	C- PGPA	Manual y procedimiento para descarga y aplicación de actualizaciones y parches.	Físico y Digital
Procedimiento De Análisis Y Tratamientos De Riesgos	GM- VR-1	Manual y procedimiento de detección, ponderación y tratamientos de Riesgos.	Físico y Digital
Procedimiento de la Red	C- CMUR	Manual y procedimiento para configuración, mantenimiento y utilización de la red.	Físico y Digital
Procedimiento Para Adquisición Desarrollo Y Mantenimiento De Sistemas	PC- PADM	Manual y procedimiento para normar la adquisición, desarrollo seguro y mantenimiento para el uso y mejora de los sistemas informáticos	Físico y Digital
Procedimiento Para Configuración De Parámetros De Seguridad	PC- PCPS	Manual y procedimiento para implementar un esquema de seguridad en la infraestructura de misión crítica	Físico y Digital
Procedimiento Para Teletrabajo	PC- PTT	Procedimiento para los permisos e implementación de Teletrabajo para el usuario final.	Físico y Digital
Procedimiento De Gestión De Cambios	PC- PGC	Manual y procedimiento para gestionar el ciclo de vida de los cambios y procedimientos que podrían representar riesgos para los activos informáticos en el uso y desarrollo de las Tecnologías de la Información	Físico y Digital
Procedimiento Para Gestión De Vulnerabilidades	PC- PGV	Manual y procedimiento para la búsqueda y gestión de vulnerabilidades de seguridad en la infraestructura tecnológica y red de datos.	Físico y Digital
Plan De Capacitación	PC- PCSI-1	Plan para la orientación y distribución de información a los empleados para el cumplimiento de las políticas de seguridad de la información.	Físico y Digital