DECLARACIÓN DE POLÍTICAS DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

El objetivo de esta declaración, es notificar a todo el personal interno y externo los principios, hábitos, buenas prácticas y recomendaciones que deberá cumplir durante la estancia en ECD.

2. POLÍTICAS DE SEGURIDAD

2.1. Todo personal a su ingreso deberá registrarse a través del sistema biométrico.

Personal operativo (Ejecutivos telefónicos):

a. Se prohíbe el ingreso a la operación con libretas, hojas, o cualquier otro material de transcripción de información.
b. No se permite el ingreso con equipos de cómputo, celulares, cámaras, y o cualquier otro activo que procese o almacene información.
c. No se permite el acceso y permanencia en las instalaciones con gorras, gorros y lentes obscuros.
d. Queda prohibido acceder a sitios de esparcimiento web (no justificados), a través de las herramientas o activos provistos por la organización.
e. No se permite el acceso con alimentos y/o bebidas a las áreas de trabajo.
f. Respetar la restricción de acceso aquellas zonas ajenas a tus estaciones de trabajo.
g. Si el personal operativo tiene consigo algún equipo de cómputo, dispositivos móviles, equipos de almacenamiento, etcétera, deberá de resguardarlo en su locker.
   NOTA: Notificar al CISO (integrante de Seguridad de la Información).
h. Todo incumplimiento de los puntos anteriores será acreedor a una sanción y/o retiro parcial del activo.

Personal administrativo:

i. Las restricciones mencionadas en el punto 2.1, del inciso “a” al “d”, serán acorde al puesto y por lo tanto a la “**RH-SI-DA08 MATRIZ DE PRIVILEGIOS DE SEGURIDAD Y ACCESO**”.

3. RESPONSABILIDADES DEL USUARIO

3.1. Las siguientes responsabilidades deberán ser adoptadas por el personal de ECD.

a. Dar cumplimiento a las responsabilidades descritas en el punto 2.1. (desde el inciso “a” al “h”).
b. Deberás bloquear tu equipo siempre que te retires de él.
c. No compartir contraseñas y accesos.
d. En caso de requerir la salida de un activo se deberá gestionar la autorización a través comité de Seguridad de Información y llenar **TI-SP-FO07 FORMATO DE SALIDA DE ACTIVO.**

e. Apego a las recomendaciones del buen uso de activos, mencionados en la Platica de Seguridad de la información y **RH-TI-SP-FO05 FORMATO DE RESPONSIVA DE ACTIVO.**

f. Acatar las recomendaciones para la prevención del COVID, dispuestas por ECD. Acatar las recomendaciones de seguridad, movimiento y evacuación compartidos porel guardia de seguridad privada.

4. APLICABLES A PERSONAL EXTERNO

4.1. ECD identifica a sus clientes, proveedores, socios de negocio, asesores, visitantes, candidatos, etcétera. Como personal externo, por tanto, deberán apegarse a las siguientes recomendaciones:

a. Toda visita deberá registrarse en la "Bitácora de Visitantes" y dejar su identificación, misma que será devuelta al retirarse de las instalaciones.

b. Toda visita deberá portar su gafete durante su estancia en las instalaciones.

c. El personal externo que requiera ingresar a las instalaciones con equipo de cómputo, dispositivos móviles, equipos de almacenamiento, cableado, herramientas u otros activos que por su naturaleza tenga contacto con los medios de procesamiento o de almacenamiento, deberán cumplir con las siguientes condiciones:

- Deberá notificar y solicitar formalmente la autorización correspondiente para su acceso o visita a ECD, a través de la persona que lo recibirá, quien por correo electrónico y mensajería electrónica gestionará la solicitud al **comité de seguridad de la información y/o SGC.**
- En el correo electrónico de visita deberá contener:
  - Número de personas
  - Equipos que ingresaran.
  - Si requieren alguna conexión u otro servicio.
  - Tiempo aproximado de estadía dentro de las instalaciones.
  - Si requiere estacionamiento (modelo del auto, color y placas)
  - Si requiere tomar fotografías, grabaciones de audio y/o videos dentro o fuera de las instalaciones (incluir especificación).

  NOTA: Revisar el **RH-SC-PG08 PROCEDIMIENTO GENERAL PARA LA AUTORIZACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**.

d. El personal externo deberá estar acompañado en todo momento por la persona a la cual visita.

e. Toda solicitud de conexión que implique el acceso a una red deberá estar autorizada por el director de TI (miembro del comité de Seguridad de la Información).

f. No podrá sustraer ningún material, equipo, documentos u otros activos que contengan información de las actividades, procedimientos, roles, privilegios, servicios, productos y/o cualquier otro tipo de información considerada restringida o confidencial sin autorización (avalada por el comité de Seguridad de la Información), caso contrario se actuará conforme a la ley y remitirá a las autoridades.

g. Acatar las recomendaciones de seguridad, movimiento y evacuación compartidos por el guardia de seguridad privada.
h. Acatar las recomendaciones para la prevención del COVID, dispuestas por ECD.
i. Todo proveedor que realice algún trabajo o actividad parcial dentro de la empresa, deberá apegarse a las prácticas y criterios operativos de Calidad, higiene y Seguridad, además de los protocolos de seguridad de Información desarrolladas por ECD.

5. POLITICAS DE PROVEEDORES

ECD considera a sus proveedores como aliados estratégicos para la prestación final de sus servicios, por tanto, se deben apegar a las siguientes políticas:

a. Establecer relaciones basadas en la honestidad y compromiso de obligaciones y acuerdos de ambas partes.
b. Aliarse con proveedores que cuenten con la infraestructura y capacidad necesaria para asegurar que la continuidad de nuestras operaciones no se vea afectadas y que en caso de afectaciones cuenten con un protocolo eficiente para la recuperación del servicio ofertado.
c. Buscar el menor coste en los suministros tercerizados, no considerando sólo el precio, sino el coste de la calidad del servicio/producto en relación su diferenciador al valor agregado para su adquisición.
d. Relacionarse con proveedores que cuenten con certificaciones en materia de Calidad o en su defecto cuenten con buenas prácticas basadas en dicha materia para la prestación de sus servicios.
e. Nuestros proveedores son evaluados semestralmente en función del cumplimiento de acuerdos, obligaciones, políticas, calidad del servicio/producto y la atención post venta.
f. En casos aplicables, establecer con los proveedores la manera de revisar, monitorizar y evaluar el servicio para efectos de medir la calidad y correcta prestación de los servicios contratados

6. LINEAMIENTOS DE ÉTICA PARA CLIENTES, PROVEEDORES Y SOCIOS DE NEGOCIO

a. Actuar de forma transparente e integra de conformidad con el marco legal aplicable en términos de fiscales y de seguridad de la información.

b. No ofrecer, aceptar o sugerir a los colaboradores directa o indirectamente pagos en efectivo, transacciones bancarias u otros beneficios para obtener una ventaja indebida o distinta a lo acordado a en el contrato comercial.

c. No aceptar, solicitar o sugerir la prestación de servicios profesionales directos o indirectos de los colaboradores de ECD.

d. Se deberá notificar a la empresa de cualquier conflicto de intereses que afecten la relación comercial o los acuerdos establecidos.

7. REPORTE DE INCIDENTES

Para el reporte de incidentes se debe cumplir el principio de “aviso a la autoridad superior”, el cual consiste en notificar a su jefe inmediato y/o al CISO, cuando se presencie un evento de riesgo de Seguridad de la Información.

8. CANALES DE COMUNICACIÓN

Cualquier comentario, duda u opinión, podrán dirigirla la siguiente dirección de correo:

- **sgcs_ecd@ecd.mx**
- **servicio_no_conforme@ecd.mx**
- **buzon@ecd.mx**

NOMBRE Y FIRMA
Mtro. Israel Ricaño
Director General

NOMBRE Y FIRMA
Lic. Guadalupe Torres
Chief of Staff

NOMBRE Y FIRMA
Mtro. Miguel Consuegra
Director de Recursos Humanos

NOMBRE Y FIRMA
Lic. Dánae Murguía
Directora de Operaciones

NOMBRE Y FIRMA
Ing. Jorge López
Director de TI

NOMBRE Y FIRMA
Lic. Enrique Talavera
Gerente SGC

NOMBRE Y FIRMA
Ing. Paulina Rivera
Líder SGC